



MIMECAST NORTH AMERICA, INC.

SOC 2 REPORT

FOR

MIMECAST EMAIL SECURITY

**A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY,
CONFIDENTIALITY, AND PRIVACY AND CCM CRITERIA**

NOVEMBER 1, 2021, TO OCTOBER 31, 2022

Attestation and Compliance Services



This report is intended solely for use by the management of Mimecast North America, Inc., user entities of Mimecast North America, Inc.'s services, and other parties who have sufficient knowledge and understanding of Mimecast North America, Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2 MANAGEMENT'S ASSERTION	5
SECTION 3 DESCRIPTION OF THE SYSTEM	7
SECTION 4 TESTING MATRICES	56

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Mimecast North America, Inc.:

Scope

We have examined Mimecast North America, Inc.'s ("Mimecast" or the "service organization") accompanying description of its Mimecast Email Security system, in Section 3, throughout the period November 1, 2021, to October 31, 2022, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that Mimecast's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) Version 4.0.3 control specifications ("CCM criteria") throughout the period November 1, 2021, to October 31, 2022.

Mimecast uses various subservice organizations for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mimecast, to achieve the CCM criteria and Mimecast's service commitments and system requirements based on the applicable trust services criteria. The description presents Mimecast's controls, the applicable trust services criteria and CCM criteria, and the types of complementary subservice organization controls assumed in the design of Mimecast's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Mimecast is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Mimecast's service commitments, system requirements, and CCM criteria were achieved. Mimecast has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Mimecast is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and CCM criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the CCM criteria were achieved and the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved the applicable CCM criteria, and its service commitments and system requirements based on the applicable trust services criteria; and;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved the CCM criteria, and its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the CCM criteria are achieved, or the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects,

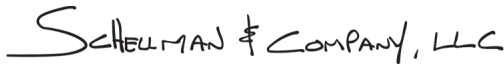
- a. the description presents Mimecast's Mimecast Email Security system that was designed and implemented throughout the period November 1, 2021, to October 31, 2022, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that the CCM criteria would be met and the Mimecast's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Mimecast's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that the CCM criteria were achieved, and Mimecast's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Mimecast's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Mimecast; user entities of Mimecast's Mimecast Email Security system during some or all of the period November 1, 2021, to October 31, 2022, business partners of Mimecast subject to risks arising from interactions with the Mimecast Email Security system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria and CCM criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

SCHEELMAN & COMPANY, LLC

Atlanta, Georgia
December 15, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Mimecast's Mimecast Email Security system, in Section 3, throughout the period November 1, 2021, to October 31, 2022, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Mimecast Email Security system that may be useful when assessing the risks arising from interactions with Mimecast's system, particularly information about system controls that Mimecast has designed, implemented, and operated to provide reasonable assurance that the criteria set forth in the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) Version 4.0.3 control specifications ("CCM criteria") were achieved and Mimecast's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Mimecast uses various subservice organizations for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mimecast, to achieve the CCM criteria and the Mimecast's service commitments and system requirements based on the applicable trust services criteria. The description presents Mimecast's controls, the applicable trust services criteria and CCM criteria, and the types of complementary subservice organization controls assumed in the design of Mimecast's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that

- a. the description presents Mimecast's Mimecast Email Security system that was designed and implemented throughout the period November 1, 2021, to October 31, 2022, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that the CCM criteria would be met and the Mimecast's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Mimecast's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period November 1, 2021, to October 31, 2022, to provide reasonable assurance that the CCM criteria were achieved, and the Mimecast's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Mimecast's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Founded in 2003, Mimecast Limited (“Mimecast” or “the Company”) offers cloud-based security, archiving, and continuity services designed to protect e-mail and deliver e-mail risk management in a single, fully integrated, subscription service. Mimecast provides protection for user entities from the threats to e-mail, and the corporate data it contains, from malware, spam, data leaks, and advanced threats (e.g., spear-phishing). Mimecast also helps organizations securely archive their growing e-mail and file repositories to support employee productivity.

The Mimecast production environment consists of software, hardware, and networking infrastructure components that support Mimecast’s Information Security Management System (ISMS). The system description in this section of the report details the Mimecast ISMS. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Description of Services Provided

Overview of the Information Security Management System

Mimecast uses a native cloud-based architecture, including a proprietary Software as a Service (SaaS) operating system and user entity-facing services to address the specific risks and functional limitations of business e-mail and data. This cloud-based approach requires no on-premises or hosted appliances to function. Mimecast provisions user entity e-mail flows and ingests e-mail data from legacy archives that drive user entity adoption and are designed to make the cloud transition more efficient for user entities. Once a user entity is live on the service, and as their requirements grow, adding new products to their subscription requires activating it from within the Company’s single, secured administration console (AdCon).

Main Services and Solutions

Mimecast Email Security

Mimecast Email Security is designed to protect inbound, outbound, and internal e-mail from malware, spam, advanced persistent threats, e-mail Denial of Service (DoS), Distributed Denial of Service (DDoS), data leaks, and other security threats. Inbound e-mail is directed through Mimecast’s Secure Email Gateway (SEG), which performs security checks before the e-mail is delivered to the user entity’s infrastructure. This prevents unwanted and potentially harmful e-mail from reaching the user entity’s environment and end users.

Outbound e-mail sent from the user entity also passes through Mimecast and is checked before being sent on to recipients in order to prevent it from presenting a security threat to the recipient. Data leak prevention services also allow outbound e-mail to be encrypted and scanned by Mimecast’s content controls to prevent confidential documents or data from inadvertently or intentionally leaving the business.

Additional Security Services Offered

- **Targeted Threat Protection (TTP)** helps protect against targeted attacks including ransomware, impersonation, and spear-phishing e-mails that infiltrate organizations, exploit users, and steal IP and user entity data. Mimecast’s TTP extends traditional gateway security to help protect organizations against these advanced and highly targeted attacks. A threat dashboard and notification system provides real-time data, including audit and reporting, enabling administrators and security specialists to monitor and report attempted attacks. TTP is the overarching brand name that includes URL Protect, Attachment Protect, Impersonation Protect, and Internal Email Protect.
- **URL Protect** tackles the threat of e-mails containing malicious links. By rewriting all URLs to point to a Mimecast service, URL Protect checks links each time they are clicked, preventing employees from visiting compromised websites regardless of what device they are using. It also includes user awareness capabilities so IT teams can raise the overall security awareness of their users. Once the user awareness

feature is enabled, a percentage of links in e-mails clicked by a user will open a warning screen. The warning screen will provide more information about the e-mail and destination, prompting them to consider whether the page is safe. If the user chooses to continue, the choice is then logged and URL Protect scans the link and blocks access if the destination is unsafe. User administrators can adjust the frequency of these awareness prompts to ensure employee caution is maintained. Repeat offenders that click bad links can be configured to receive more frequent prompts until their behavior changes. The user IT team can track employee behavior from the Mimecast AdCon and target additional security training, as required.

- **Attachment Protect** reduces the threat from weaponized or malware-laden attachments used in ransomware, spear-phishing, and other advanced attacks. It includes preemptive sandboxing to automatically check e-mail attachments before they are delivered to users. Attachments are opened in a virtual environment or sandbox, isolated from the corporate e-mail system, security checked, and passed on to the user if no threat is detected. Attachment Protect also includes the option to convert attachments into a safe file format, neutralizing malware in the process and delivering the mail and attachment without the typical sandbox delays. The attachment is delivered to the user in read-only format. Should the employee need to edit the attachment, they can request it, and it will be sandboxed on-demand and delivered in the original file format.
- **Impersonation Protect** tackles the threat of malware-less social engineering-based e-mail attacks, often called CEO fraud, impersonation, whaling, or business e-mail compromise. As e-mail passes through the Mimecast SEG, Impersonation Protect examines several key aspects of the message (i.e., indicators of compromise). If the e-mail fails a configured combination of these tests, administrators can configure Impersonation Protect to discard the message, quarantine it, or notify end users that the e-mail is suspicious.
- **Internal Email Protect** helps reduce the risk of a breach or damaging security incident spreading throughout the organization. By analyzing internal e-mail through a journal feed, Mimecast can detect lateral movement of attacks via e-mail from one internal user to another. This allows organizations to monitor, detect, and remediate e-mail-borne security threats that originate from within their e-mail systems, whether the e-mails are destined for other internal users or external recipients. Internal Email Protect includes the scanning of attachments and URLs for malware and malicious links, as well as content filtering enforced by Data Leak Prevention services. In addition, Internal Email Protect includes the ability to automatically delete infected e-mails and attachments from employees' inboxes.
- **Secure Messaging** allows employees or administrators to initiate secure e-mail delivery directly from the e-mail client. Policies can be configured by the administrator to be applied automatically at the gateway or by employee selection within Outlook and other Mimecast desktop and mobile applications on outbound e-mails. Configurable options include setting the expiration date, read receipt, and no print / reply / forward options. Mimecast Secure Messaging is a secure and private channel to share sensitive information with external contacts via e-mail without the need for additional user entity or desktop software.
- **Large File Send** enables PC and Mac users to send and receive large files, up to 2GB in size, directly within Outlook, a native Mac application, or the Mimecast Personal Portal (web application) and means users are no longer constrained by e-mail size limits imposed by their IT team or e-mail infrastructure. Mimecast Large File Send protects attachments in line with user entity-driven security and content policies by utilizing encryption, optional access keys, and custom expiration dates. Mimecast Large File Send also supports audit, e-discovery, and compliance requirements by archiving files and notifications according to user entity e-mail retention policies. It also helps protect e-mail system performance from the burden of large file traffic.

Mimecast Email Incident Response (MEIR)

Mimecast Email Incident Response (MEIR) lowers the dwell time of cyber security threats and reduces the burden on customers SOC, of e-mail threat response and remediation. User reported threats are routed to Mimecast's SOC where they are automatically analyzed, triaged, and prioritized for expert analyst classification and remediation. MEIR use automation including AI to rapidly triage and prioritize reported e-mails for automatic remediation and universal blocking. For any unknown e-mail, manual investigation by Mimecast SOC analysts takes place. In addition, Mimecast applies a universal blocking of all newly discovered threats. The malicious e-mail is also remediated from the customer's environment either via automatic remediation or via manual remediation conducted by Mimecast's SOC analysts.

Mimecast Mailbox Continuity

The Mimecast Mailbox Continuity service protects against on-premises, cloud, and hybrid primary e-mail system downtime with always-on e-mail access for employees via desktop, web, and mobile applications. It allows user entities to avoid downtime because of an outage or planned maintenance, without the need to replicate their own infrastructure in a second location. Mimecast provides secure and uninterrupted access to live and historic e-mail and attachments as well as to calendar information from the Mimecast Cloud using tools like Outlook for Windows, the web, and mobile applications.

As all user entity outbound and inbound e-mail is flowing through Mimecast, when the user entity's primary e-mail service is unavailable, Mimecast Mailbox Continuity service takes over the delivery and sending of e-mail in real-time at the request of the administrator, offering rapid fail-over and fail-back capabilities. Continuity Event Management features further facilitate outage handling by providing a monitor service that sends a message probe from the user entity's server to determine availability. A configured threshold triggers an administrative alert when reached and provides a temporary event portal for an administrator to invoke 'continuity mode', notify end users, or suppress further alerts.

Mimecast Enterprise Information Archiving

The Mimecast Enterprise Information Archiving service offers storage of e-mail, files, and instant messaging conversations paid for on a per-user basis. Onsite archives can be decommissioned, reducing the data load on the primary e-mail service. Legacy data can be ingested via Secure File Transfer Protocol (SFTP) or via encrypted physical drives sent from the user entity to Mimecast.

Mimecast has the ability to save e-mail, file attachments, and associated critical metadata that identifies if an activity is sent or received. The mobile, desktop, and AdCon search tools allow for a detailed review of the archive. Mimecast also enables user entities with legacy archive data to put information into a single archive with a complete historical view. Mimecast Enterprise Information Archiving provides an easy-to-manage, fully indexed, immutable storage for administrative e-discovery and rapid employee access with a seven-second search service-level agreement (SLA). As an independent archive from primary mail systems, data can be verified and moved easily if a change to the primary mail server is necessary.

Web Security

Mimecast Web Security is a cloud-based service that protects against malicious web activity initiated by user action or malware (e.g., ransomware and other malicious software). The solution also provides protection against unsanctioned cloud application use ("Shadow IT") through its Application Visibility & Control functionality.

Based on configuration, the web or application DNS request is forwarded to the Mimecast service for inspection and resolution or filtering. The Web Security product blocks access to malicious or business-inappropriate websites or applications based on customer policy. A software agent is available for off-network roaming devices and provides additional capabilities such as direct IP communication reporting and blocking. Mimecast Web Security uses the same technology as the Targeted Threat Protection suite. When combined with the Mimecast Secure Email Gateway, the Web Security product protects organizations against the two dominant cyberattack vectors: e-mail and the web.

Mimecast Browser Isolation

Mimecast Browser Isolation can be deployed as a layer of security to complement Mimecast Web Security and Email Security's URL Protect. With Mimecast Browser Isolation, when a user attempts to access a website that is new and uncategorized, the target web page is accessed by a browser running in an isolated container on a secure server in the Mimecast cloud.

Web pages are safely streamed from the Mimecast cloud to the user's browser. To ensure minimal impact on bandwidth and computer performance, video is X264-encoded; streamed at a variable bitrate based on available bandwidth; and rendered in the user's browser using a proprietary, secure, and lightweight communications protocol. For some websites, the bandwidth consumed by video streaming can be less than that for direct download. Mimecast Browser Isolation can be configured in read-only mode, which prevents the user from typing and pasting data into web forms or uploading files. This blocks phishing attempts for credentials and other sensitive information, as well as malicious or unintentional loss of information.

Mimecast Awareness Training

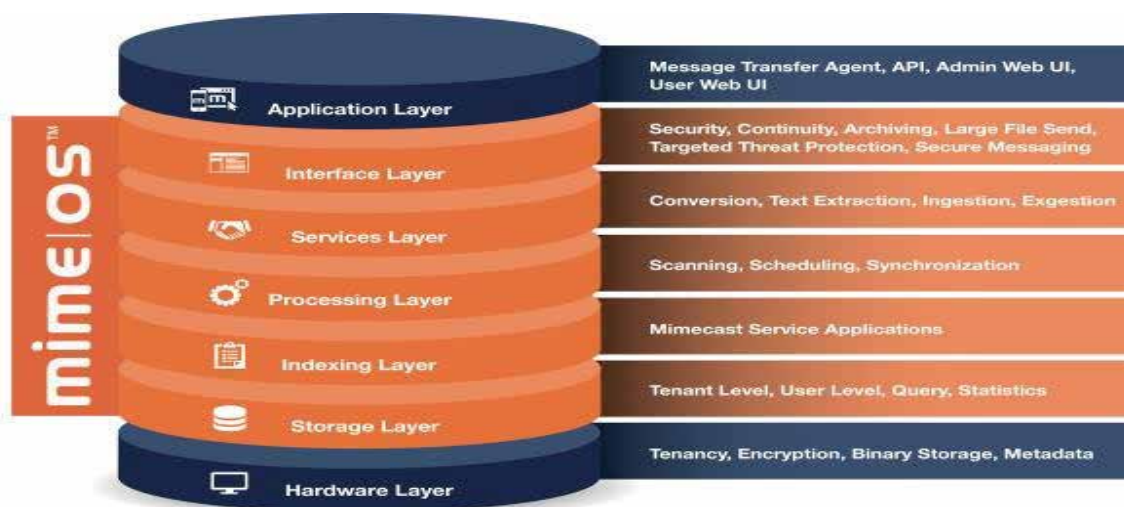
Mimecast Awareness Training is an integrated security awareness training and cyber risk management platform that helps organizations understand and mitigate their overall risk relative to their peers. The intelligence gained from the solution becomes a key part of Mimecast SAFE Score which enables the unlocking key indicators of human error and enables monitoring of human behavior over time. As well as providing a library of phishing templates to use for training, SAFE Phish enables real phishing attacks targeting an organization to be easily converted into de-weaponized phishing simulations. The Awareness Training video modules can be provided as a SCORM solution for customers wanting to maintain employee training programs within their Learning Management System.

The Global Data Center Network

Mimecast has built a network of sixteen data centers in seven locations around the world to deliver its SaaS. This allows user entities to address their data management and protection requirements with geographic and jurisdictional control over where their data resides. Each region operates two identical but geographically disparate data centers, functioning in an active-active configuration and replicated in real time. In the event of a data center failure or planned maintenance, Mimecast is able to failover full operations to the healthy data center to maintain the user entity's e-mail and data services.

Proprietary Native Cloud Architecture – Mime OS

Mimecast has developed a proprietary operating system for cloud services called Mime OS. Mime OS enables a secure, multi-tenancy environment that uses hardware specifically for the secure management of e-mail and data. Mime OS is the proprietary operating system that controls the interface, services, processing, indexing, and storage layers of Mimecast's cloud architecture.



Mime OS uses a common code base to control the interface, services, processing, indexing, and storage layers of Mimecast's cloud architecture. It is designed to enable scale in storage, processing, and services to meet large enterprise-level e-mail and data demands while retaining the cost and performance benefits of a cloud environment. Mime OS is designed to streamline Mimecast user entity application development and enable integration across services. User entity applications or API services use Mime OS to interact with Mimecast's data stores and processing technology.

Continuous Development Methodology and Multi-Tenancy

As Mimecast enhances and expands its SaaS technologies, services are updated centrally with no user entity impact and no user entity intervention required. All user entities share the same core operating and application software. As a result, improvements, upgrades, new products, or patches are applied once and are then immediately available to the entire user entity base.

Mimecast's focus on the continual improvement of Mime OS allows for constant advancement of the performance and capabilities of the SaaS environment. These improvements include faster archive search times, quicker data ingestion, greater storage density, improved processing performance, and enhanced security controls. Additionally,

when threat intelligence is gathered and new threats emerge, Mimecast adapts its ISMS to benefit all user entities. Mimecast can also identify and act on threats to one user entity and quickly prevent them from impacting others by updating the core system.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the Mimecast ISMS. Commitments are communicated via the Company's General Terms and Conditions, and its Cyber Resilience and Web Security Technical and Organizational Security Measures online.

The Company's principal service commitments related to Mimecast ISMS include the following:

- Manage the assessment and treatment of risks to continually improve Mimecast ISMS' information security.
- Protect the physical assets that contain customer data.
- Ensure systems containing customer data are used only by approved, authenticated users.
- Ensure personnel entitled to use systems gain access only to the customer data that they are authorized to access.
- Ensure customer data is not read, copied, altered, or deleted by unauthorized parties during transfer or storage.
- Ensure customer data remains confidential throughout processing and remains intact, complete, and current during processing activities.
- Ensure that customer data is protected from accidental destruction or loss and that there is timely access, restoration, or availability to customer data in the event of a service incident.
- Ensure each customer's data is processed separately.
- In the event of any security breach of customer data, ensure the effect of the breach is minimized and the Customer is promptly informed.
- Ensure Mimecast regularly tests, assesses, and evaluates the effectiveness of the technical and organizational measures.
- Maintain appropriate administrative, technical, and physical security measures to protect customer data against unauthorized access, disclosure, and loss.
- Comply with the applicable laws and regulations of the Hosting Jurisdiction, including without limitation, as applicable, the UK Data Protection Act 1998 and the US Health Insurance Portability and Accountability Act.
- Ensure Mimecast will: (i) use a Disclosing Party's confidential information solely for the purpose of its performance of the activities; (ii) disclose such information only to its employees, agents, and contractors who are bound by obligations of confidentiality; and (iii) protect the Disclosing Party's confidential information against unauthorized use or disclosure using the same degree of care it uses for its own confidential information, which in no event will be less than reasonable care.
- Mimecast shall only Process Personal Data on behalf of Customer in accordance with and for the purposes set out in the Instructions, which, for the avoidance of doubt and depending on the Services provided, may include Mimecast (i) providing the Customer with access to and use of the Services; and (ii) if applicable, improving and developing the Services, including but not limited to using Threat Data to train the Service's machine-learning algorithms, the output of which are anonymized and irreversible. Notwithstanding the foregoing, Processing may be required by Union or Member State law to which Mimecast is subject. In such a case, Mimecast shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

- Mimecast shall notify Customer without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) of a declared breach of security which has led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer's Personal Data which affects the integrity, availability or confidentiality of Customer's Personal Data ("Security Breach"). For the avoidance of doubt, Security Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems and no notice of the foregoing shall be required. In the event a Security Breach requires notification by Customer to Data Subjects or relevant Regulators, the parties agree to coordinate in good faith on developing the content of any public statements or required notices.
- Customer hereby consents to the use of the Third-Party Subcontractors to perform Services. Subcontracting for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the principal obligation related to the processing of Personal Data pursuant to the Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Mimecast agrees that it has a written agreements in place with all Third-Party Subcontractors that contains obligations on the Third-Party Subcontractor that are no less onerous on the relevant Third-Party Subcontractor than the obligations on Mimecast under this DPA in respect of the specific Services provided by the Third-Party Subcontractor.
- If Mimecast appoints a new Third-Party Subcontractor or intends to make any changes concerning the addition or replacement of the Third-Party Subcontractors, it shall provide Customer with reasonable advance written notice. For the purposes of this Clause 8.2, notice may be provided electronically, including but not limited to posting on the Mimecast administrative console of the Services, a notice on the Trust Center and/or in a e-newsletter sent to Customer (if Customer has subscribed to such e-newsletter via Mimecast's online preference center). If Customer objects to the appointment or replacement of Third-Party Subcontractor in writing based on legitimate data protection grounds within ten (10) days after Mimecast's advanced written notice of a new Third- Party Subcontractor.
- Mimecast shall provide reasonable assistance in response to inquiries from Customer or its Regulator relating to Mimecast's Processing of Customer's Personal Data. Mimecast shall, upon written request from Customer, provide Customer with information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor.
- Upon termination of this DPA in accordance with Clause 11, Mimecast shall, at Customer's request: delete all Personal Data Processed on behalf of Customer, unless applicable laws, regulations, subpoenas or court orders require it to be retained; or assist Customer with the return to Customer of Personal Data and any copies thereof which it is Processing or has Processed upon behalf of Customer. Customer acknowledges and agrees that the nature of the Services mean that Customer may extract a copy of Personal Data at any time during the term of the Agreement.

System requirements are specifications regarding how Mimecast ISMS should function to meet the Company's commitments to customers. System requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements related to Mimecast ISMS include the following:

- Logical access standards
- Physical access standards
- Employee provisioning and deprovisioning standards
- Access reviews
- Encryption standards
- Intrusion detection and prevention standards
- Risk and vulnerability management standards
- Configuration management

- Incident handling standards
- Change management standards
- Vendor management

In accordance with Mimecast's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

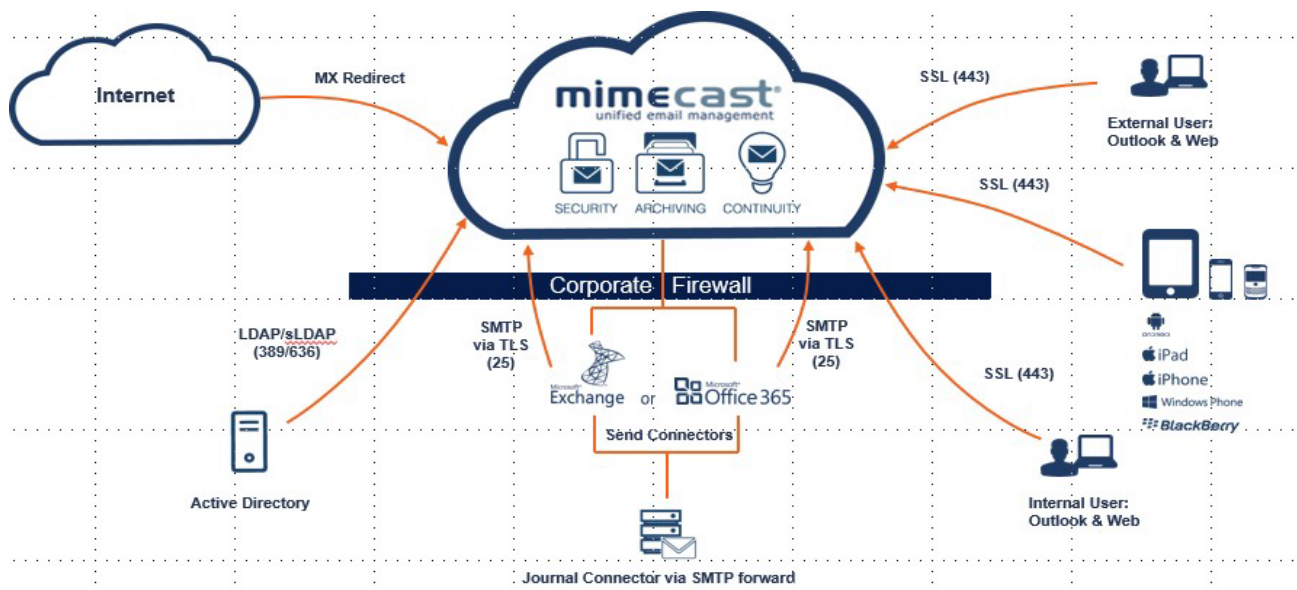
A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Mimecast's production environment consists of the hardware, software, and networking used to deliver the SaaS environment. Hardware and software residing at Mimecast office locations is not relevant to the delivery of Mimecast end user services. For example, Mimecast general office support software or hardware that is only used for Mimecast internal purposes are outside the boundaries of the system for providing Mimecast's SaaS environment. Mimecast offices do not host applications or infrastructure critical to the operation of the Mimecast production environment and are out of the scope of this report.

There are other hardware and software components that indirectly support the mission of Mimecast in terms of the services described in the section titled "Main Services and Solutions" above. However, these components are materially insignificant to the design and operation of ISMS controls described in this report. For the purposes of this report, Mimecast included all network, hardware, and software that support the SaaS environment. Note that while some Mimecast user entities must download and install Mimecast user entity software on their devices (such as their laptops, workstations, servers, or mobile devices), those hardware devices and the protection mechanisms and controls provided by user entities are beyond the scope of this report.

[Intentionally Blank]

Infrastructure and Software



Hardware

The underlying hardware infrastructure supporting Mimecast's SaaS environment includes branded as well as white-labelled servers, assembled in line with Mimecast's custom specifications. Direct-attached storage is used on each processing host. Servers are arranged in high-density racks, with redundant switches in each rack connecting the servers to a redundant core switch. Power is fed to each server across two independent circuits. In order to provide high availability in the event of server hardware or data center failures, redundant server hardware is deployed across both data centers in each region.

Software

Mimecast uses a combination of commercial off-the-shelf (COTS) software, open-source software, and proprietary code for providing services to its user entities and maintaining its operations. Mime OS has been developed by Mimecast, specifically for the provision of secure management of e-mail and data to its user entities. Mimecast's Technical Operations department uses a combination of open-source monitoring software and custom-built software to monitor its global operations. These tools are used to monitor the operating systems, hardware, applications, and networking infrastructure that make up Mimecast's SaaS environment. These tools also provide performance, throughput, and other relevant metrics, enabling Mimecast to measure adherence to its SLAs.

Networking

Mimecast's network was designed to protect the security, availability, processing integrity, confidentiality, and privacy of user entities' data traversing the network. Mimecast has designed and implemented a switched fabric network, which has servers connected via redundant switches to form a meshed network for higher throughput and continuous availability. This is achieved through redundant core switches and redundant top-of-rack edge switches. Wide Area Network (WAN) and Local Area Network (LAN) interfaces are physically separated on the Mimecast production infrastructure. Event logging is configured on all firewalls. These logs are sent to the Mimecast Security Information and Event Management (SIEM) system for correlation, analysis, and secure storage.

Mimecast has implemented network segmentation using virtual local area networks (VLANs), with access control lists configured to create a collection of segregated networks within the data centers. VLAN segmentation improves network manageability and security by decreasing access to systems, thereby reducing attack surfaces and making it more difficult for threat agents to traverse the internal network. In addition, using VLAN segmentation, authorized users and devices are only able to access the servers and devices necessary to perform their daily tasks. Data in transit between user entity systems and Mimecast's web applications is encrypted using Transport Layer Security (TLS), a cryptographic protocol that protects the privacy and integrity of the data as it passes through the network. Mimecast's administrators are required to use an encrypted VPN with two-factor authentication to connect to Mimecast's internal network.

Mimecast's SaaS components reside in colocation data centers operated by Cyxtera (CenturyLink), NaviSite, Telstra, Equinix, Macquarie, Internet Solutions, e-shelter, Cologix, Databank, NTT and Sure International in seven regions (US, South Africa, UK, Germany, Australia, Canada, and British Channel Islands). These colocation providers were chosen based on requirements for availability, survivability, security, confidentiality, safety, and manageability.

People

The Company develops, manages, and secures the Mimecast ISMS via separate roles. The responsibilities of these roles are defined as follows:

- **Corporate:** Includes Executive Management; the Chief Security & Resilience Officer (CSRO); Technical Operations management and staff; and supporting staff from functions including Assurance Risk and Controls (ARC), Legal, Finance, and HR.
- **Security Committee, Organizational Resilience Committee, and the Enterprise Risk Management Committee:** Accountable for providing regular updates to the Board of Directors. There is also a comprehensive Internal Audit program which provides an Audit Plan to Executives for review and approval. The CEO is a permanent and active member of the monthly Security Committee meetings.
- **Technical Operations, Engineering, and Service Delivery:** Includes staff that administer the e-mail continuity, archiving, and security service. They provide the direct day-to-day services, such as management of user entity data environment, information security, technical operations, software development, and user entity service and communication.

The Company departments directly concerned with security:

- **Security:** Responsible for the implementation and authorization of security policies; controls and procedures; security-focused strategic direction; security awareness; and technical security activities such as penetration testing, secure design of systems, technical audits of hardware and software, and code review at an operational level. The CSRO is directly accountable for security and organizational resilience oversight and the efficacy of security control design and implementation.
- **ARC:** Responsible for Governance, Enterprise Risk Management, Technical Audit and the Attestation, Certification, and Assessment (ACA) program. The Vice President of ARC is accountable for risk oversight and the efficacy of entity-level risk control design and implementation.
- **Engineering:** Responsible for secure software development, software quality assurance, and operational implementation of identified controls.
- **Technical Operations:** Responsible for securing the technical infrastructure in relation to user entity data, systems that support logical and physical access to user entity data, data center management, and operational implementation of identified controls.
- **IT:** Responsible for systems that support logical and physical access to IT systems, telecommunications, administrative systems, and physical access to Mimecast facilities.
- **HR:** Responsible for credentialing (background checks) and operational implementation of human capital controls, including job descriptions, security learning, and the administration of employment contracts and non-disclosure agreements.

Product Management: Responsible for the product planning and execution throughout the product lifecycle. This includes ensuring the products are assessed for security and privacy implications and support the company's strategy and goals.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Mimecast ISMS. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are

drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business.

The following list details the procedures as they relate to the operation of the Mimecast ISMS:

- Logical and Physical Access - how the Company restricts logical and physical access, provides, and removes that access, and prevents unauthorized access.
- System Operations - how the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
- Change Management - how the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
- Risk Mitigation - how the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Information Security

The policies, standards, processes, and procedures implemented by Mimecast to ensure the security, availability, confidentiality, processing integrity, and privacy of the SaaS environment are made available in the Mimecast ISMS and described in detail in the Information Security Policy. The Mimecast ISMS sets the overall framework for managing the security of Mimecast's information technology environments. The CSRO is accountable for interpreting these policies and developing appropriate standards. Management is accountable for ensuring procedures that describe the operational implementation of required controls are documented and enforced.

User Entity Account Management

Mimecast creates the first user entity administrator account when the user entity account is initially set up. The credentials are shared securely with the designated technical contact at the user entity. User entities are then responsible for administering user access to their environment either manually or through directory synchronization.

User Entity Access Control

User entities typically integrate their Mimecast account with their Active Directory (AD) environment using Integrated Windows Authentication (IWA). Two-factor authentication is supported using Security Assertion Markup Language (SAML). Cloud or local passwords can also be created in the Mimecast Platform by the user entity administrator. User entities can create Authentication Profiles to apply various combinations of authentication types to groups of users to suit their own requirements.

If a username and password are used:

- Password requirements are controlled by the user entity. These include minimum length and complexity requirements such as lower case, upper case, numeric, and special characters. They also control the expiration, lockout threshold, and lockout duration of their users' accounts.
- For user entities that utilize their own AD environment to authenticate users, it is the responsibility of the user entity's Administrator to define the username and password requirements in their own AD environment and communicate those requirements to their users as they deem appropriate.
- Changing a password in AD changes the password a user would use to log onto Mimecast's services. If the user entity uses cloud passwords, the administrator can change the password in the AdCon in the user's account configuration.

Cloud passwords are stored in a database, salted, and hashed:

- User session timeouts are configurable by the user entity and can range between 20 minutes and 12 hours.

User Entity Roles

Roles are used to provide access rights for those who need to access the Mimecast AdCon. The role determines the depth of access and can be used to control the tasks that can be performed by an Administrator. Custom roles can be created by the user entities' Administrators to provide granular, administrative permissions control. New or

existing user access change requests that will result in access to a high value 'restricted' information class (e.g., user entity data) are additionally reviewed by the Mimecast Security Team.

User Entity Audit Logging and Monitoring

Every account has an Event Log accessible from the AdCon. The Mimecast Administrator logs into the AdCon and modifies accounts under the directory section. The AdCon acts as an auditor of relevant administrator, user, or automatic activities within the account. Actions that are logged include the following:

- Account changes
- User account changes (including password changes)
- New policies or deleted policies
- Any definition or policy amendments
- Directory synchronization
- Journal failures
- Folders being created or updated
- User login attempts and failures

E-mail flow and queues are also monitored, logged, and made available via the AdCon. These logs include the following:

- Message Track and Trace – messages that are sent or received through Mimecast are logged when they are accepted.
- Attachments – any attachment that is blocked or stripped and linked from an e-mail.
- Connections – connection attempts made to the user's Mimecast account that are not initially accepted.
- Delivery – queue of all e-mails (inbound and outbound) on retry or waiting to be delivered by Mimecast.
- Held – e-mails being held in Mimecast due to policies based on spam scanning, content, or attachment-based policies.
- Rejections – all e-mails that have been rejected in protocol by Mimecast security systems; has a seven-day rolling log.
- System – current notifications that are being processed and queued.
- TTP – a class of security measures that includes URL and e-mail attachment protection. The logs available to the user entity via the AdCon show TTP activity on their account.

User entities have access to the logs through the AdCon. User entities can generate reports to be sent at intervals to appoint administrators or run reports based on criteria and export to charts or spreadsheets. Administrators can also monitor logs in real time via the AdCon. The logs are “read only,” and there is no option to delete a log. User entities can also integrate these logs into their existing SIEM via an API.

Mimecast's Internal Access Control

Access rights for information system assets are primarily allocated via AD and Lightweight Directory Access Protocol (LDAP) security groups. New or existing user access change requests that will result in access to a high value 'restricted' information class (e.g., user entity data) are additionally reviewed and approved by the user's manager and Security Team before access is granted. Password complexity standards are implemented. Two-factor authentication and the use of encrypted VPN channels are mandatory to gain remote access to IT system components. Mimecast's policies prohibit employees sharing account details.

During on-boarding or off-boarding, user accounts are created or disabled in AD, VPN systems, and other supporting services. The employment start or termination date triggers the provisioning or de-provisioning of accounts. This is done via an automated feed of user changes from the HR management system into the case queue for IT. Mimecast's policies prohibit the reactivation or use of a terminated employee's AD account for any

other purpose than the return of the same employee or for operational necessity such as a line manager requiring access to the inbox of a previous employee. In that instance, a request for reactivation is made using the change management process and the account is reset with a new password before re-activation.

Mimecast's Internal Logging and Monitoring

Logging and monitoring are used to collect data from system infrastructure components and endpoint systems to monitor system performance and utilization, identify potential security threats and vulnerabilities, and detect unusual system activity or service requests. Security and system logs are stored locally on the device that generated the log and additionally sent to the Mimecast SIEM. The SIEM alerts the Security Operations Center based on a defined set of rules.

Backups

Mimecast's SaaS environment is based on a proprietary, geographically dispersed, high-availability cluster architecture. The data centers operate in an active-active configuration, and replication of data between data centers occurs in real time. Mimecast's storage environment incorporates triple redundancy to protect archived customer data. Therefore, traditional tape-based backup and recovery procedures are not required. Data is continuously replicated to primary, secondary, and tertiary storage nodes between the two data center locations. This process protects data to such a degree that the Mimecast network can automatically heal and protect itself against data loss and corruption. Alert notifications are sent to Mimecast's Technical Operations and Storage Teams when replication failures occur. Replication failures are investigated and resolved as needed. Hash-level integrity checks are performed on archived data. Replication failure recovery is performed regularly, and serious anomalies are investigated and resolved immediately.

Change Management Process

Mimecast has documented policies and procedures to guide employees making changes to the system. Change requests come from one of the three interfaces and are categorized as project, standard, or emergency changes.

Project Changes

The types of changes that are categorized as project are planned and would include major feature requests. Project-based changes are predominantly manual, and the changes move through a series of stakeholder gates where the safety of the change is assessed.

Standard Changes

The types of changes that are categorized as standard are planned and typically have a low probability of failure. The low failure assessment is based on previously successful deployments of the same change type. Standard changes are semi-automated (human intervention is part of the process), and the changes move through a series of gates where the safety of the change is assessed.

Emergency Changes

Due to the nature of emergency changes, fewer change gates are mandated to accommodate a compressed timeframe. For this reason, and because these changes are unplanned, emergency changes may have a higher probability of failure. To reduce the probability of system failure because of the change, additional resources are temporarily assigned to the change management process by convening the Emergency Management Team (EMT) as part of the incident management process. Security vulnerability testing is included in the types of tests performed on relevant application, database, network, and operating system changes. A code review or walkthrough is required for high impact changes that meet the established criteria. These are performed by a peer programmer who does not have responsibility for the change.

System and regression testing are prepared by the Quality Assurance (QA) team. Deviations from planned results are analyzed and submitted to the appropriate developer. Post-implementation regression tests, designed to verify the operation of system changes, are performed for a defined period as determined during project planning. Following the implementation of major changes, results are shared with internal and external stakeholders, where appropriate. Major changes that may affect customers require notification in advance of the change being implemented. To limit unexpected impact from changes, separate environments are used for development, QA, and production. Changes are required to be tested in the development and QA environments before being implemented in production.

Capturing Significant Events and Conditions

Mimecast has established the Organizational Resilience Committee to oversee all activities and actions associated with capturing significant events and conditions that have the potential to impact user entity-facing systems and services. Mimecast uses various monitoring tools and technologies to ensure that critical components for the delivery of services are always available. The monitoring tools are operational 24 hours a day, seven days a week, and 365 days a year, and periodic testing is done to ensure they remain effective.

In the event of any failure that impacts a production service, Mimecast activates the Business Continuity and Emergency Response Plan. All serious user entity-impacting incidents require an incident report that details the root cause analysis. This enables Mimecast to understand the reasons for failure events and prevent reoccurrence through the implementation of a corrective action plan. Mimecast provides an incident report to user entities, describing the root cause(s) of the failure and the corrective actions that will be taken to minimize the possibility of recurrence. Incident management policies and procedures stipulate how to prevent incidents and how Mimecast personnel should respond to incidents when they occur. The Information Security Policy and security awareness training address the detection and correction of incidents as they arise. Mimecast has systems and processes in place for detecting and managing security incidents. Incident management policies and procedures address incidents in all of Mimecast's environments.

When an incident is identified, an incident ticket is created with the details of the event, including the date and time the incident occurred, the nature of the incident, and how the incident impacts user entities. The ticket is assigned a priority based on the severity to the user entity, and then a multi-discipline team initiates an investigation to assess the scope and impact of the situation and to determine the actions necessary for mitigation. Mitigation includes the prevention of any continued loss of data or services, valuation of existing controls, an analysis of the event, and the required notifications of regulatory authorities or impacted entities. Service-impacting events may be detected by internal monitoring systems that monitor facilities, networks, and applications. In addition, user entities and users may directly report events.

Availability

The availability category refers to the accessibility of the system or services as committed by the Company's General Terms and Conditions Agreements, SLAs, and Customer Contracts. The availability of the Mimecast ISMS is dependent on many aspects of the Company's operations, including monitoring and scaling of critical resources. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations or during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore backed-up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but rather from routine processing errors and failures of system elements.

Mimecast has a number of controls in place to address the availability risks described above. For example, an IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. Application errors and processing capacity are monitored continuously, and the monitoring tool generates alerts when specific, predefined thresholds are met. System configuration backups are performed using an automated system and replicated across the whole production environment to provide resiliency. Archived customer data (e-mail) is replicated onto two separate servers within the same data center, and a third copy is replicated to a third server hosted within a separate data center. The

Company uses a multi-location colocation strategy that is comprised of two data centers for each jurisdiction to permit the resumption of operations at other colocation facilities in the event of a total loss of one data center. A documented business continuity and disaster recovery plan has been developed and is updated during the period. A business continuity and disaster recovery plan test is performed during the period.

Processing Integrity

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the Mimecast ISMS achieves the purpose for which it exists and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. The processing integrity criteria addresses input, processing, output, and storage of data within the Mimecast ISMS.

The Company has designed its controls to address the following processing integrity risks:

- Software or data are lost or not available due to processing error, intentional act, or environmental event
- Current processing capacity is not sufficient to meet processing requirements, resulting in processing errors
- Inputs are captured incorrectly
- Inputs are not captured in a timely manner
- Data is lost during processing
- Data is inaccurately modified during processing
- Processing is not completed within the required timeframe
- Data is not available for use as committed or agreed
- Stored data is inaccurate or incomplete
- System output is not accurate
- System output is provided to unauthorized recipients

Mimecast has a number of controls in place to address the processing integrity risks described above. For example, customer-related field forms limit an input to acceptable values for storage in the database. Customer-related field forms prevent submission if mandatory fields have not been completed. The system monitors and logs customer e-mail data when it is received, processed, and delivered. A data structure file is created for customer data when first stored. In the event of data corruption, the system automatically repairs the file using the Company's proprietary e-mail storage system. The application administration portal does not give internal personnel the ability to modify customer data.

Confidentiality

The confidentiality category refers to the protection of customer information as committed by the Company's service agreements. The confidentiality of Mimecast's system is dependent on many aspects of the Company's operations, including appropriate data encryption (at rest and in transit) and processes regarding management of data held within the system. The risks that would prevent the Company from meeting its confidentiality commitments and requirements are diverse. The Company has designed its controls to address both internal and external confidentiality risks specifically related to protection from improper use and disclosure (including monitoring of vendor services), as well as the proper retention and disposal of confidential customer information. In evaluating the suitability of the design of confidentiality controls, the Company considers the likely causes of improper disclosure or handling of confidential information and the commitments and requirements related to confidentiality.

Mimecast has a number of controls in place to address the confidentiality risks described above. For example, the Company creates test data using a test data generator. Customer data is not used for development or QA testing. Privileged access to the following in-scope system components is restricted to authorized users with a business need: the network, AdCon console, operating system, database, and firewall. A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company. Confidentiality and non-disclosure agreements are established

with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.

The Company has deployed TLS for the transmission of confidential or sensitive information over public networks. Remote access by employees is permitted only through Multi-Factor Authentication (MFA) over an encrypted VPN connection. Databases housing sensitive customer data are encrypted at rest with Advanced Encryption Standard (AES) -256 encryption. System configurations on employee workstations and laptops prevent production data from being backed up onto removable media. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments applicable to the service provided. Related third-party and vendor systems providing services to the Company are reviewed quarterly as part of the vendor risk management process. Attestation and certification reports (including SOC 2 reports) are obtained and evaluated when available. Electronic media containing confidential information is destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. The Company systematically erases confidential information to meet the Company's confidentiality commitments and system requirements. Where appropriate, hard copies of confidential information are securely shredded. Formal disposal procedures are in place to guide the secure disposal of Company and customer data.

Data

E-mails, including attachments, are stored in Mimecast's proprietary operating system, Mime OS. All user entity data is classified as "Restricted," Mimecast's highest information classification level. User entity data is stored in Mimecast's archive layer using AES-256 encryption. Keys are generated by a Federal Information Processing Standard (FIPS) 140-2 aligned key generation system. Mimecast replicates user entity data in real-time between two in-region, geographically disparate data centers. User entity data is stored in triplicate. Data retention is defined by user entities based on individual corporate policy requirements. Data input in Mimecast's applications is sanitized on the server side using character encoding before being stored in the application or submitted in a database query.

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The data center hosting services provided by Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, shelter, Cologix, Databank, and NTT were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria and CCM criteria that are intended to be met by controls at Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, shelter, Cologix, Databank, and NTT, alone or in combination with controls at Mimecast, and the types of controls expected to be implemented at Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, shelter, Cologix, Databank, and NTT to achieve Mimecast's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT	Applicable Trust Services Criteria and CCM Criteria
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.	DCS-01-DCS-14, LOG-14 CC6.4 - CC6.5

Control Activity Expected to be Implemented by Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT	Applicable Trust Services Criteria and CCM Criteria
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.	BCR-01 - BCR-05, BCR-08 - BCR-11, DCS-14 - DCS-15, DSP-19 A1.2

PRIVACY NOTICE

Mimecast provides the privacy notice to individuals about whom personal information is collected, used, retained, disclosed, and disposed of or anonymized.

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is entered into by the customer (“**Customer**”) and the applicable Mimecast entity providing the Services (“**Mimecast**”), with each of the Customer or Mimecast referred to as a party and collectively as the parties. This DPA shall form part of and is incorporated into the services agreement entered into between the parties hereto (“**Agreement**”) and is effective from the date of last signature below (the “**Effective Date**”).

By signing below, Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Law (defined hereinafter), in the name and on behalf of its Authorized Affiliates, if and to the extent Mimecast Processes Personal Data for such Authorized Affiliates and they qualify as, for the purposes of the GDPR, the controller and, for the purposes of the CCPA, the business. For the purposes of the GDPR, Mimecast is the processor and, for the purposes of the CCPA, the service provider. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the Services to Customer pursuant to the Agreement, Mimecast may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA:

This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, and 3.

This DPA has been pre-signed on behalf of Mimecast. To complete this DPA, Customer must complete the information in the signature box and sign on Page 10.

Send the completed and signed DPA to Mimecast by email, indicating the Customer’s Account Number (as set out on the applicable Mimecast Order Form or invoice), to the Customer’s applicable Customer Success Manager. Upon confirmed receipt of the validly completed DPA by Mimecast, this DPA will become legally binding.

HOW THIS DPA APPLIES:

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Mimecast entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA is neither a party to a Services Order nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

For the avoidance of doubt, if a Services Order or an Agreement does not exist between Mimecast and a party signing this DPA on behalf of Data Controller, this DPA is not valid and of no force and effect.

The Mimecast entity that has entered into the applicable Services Order or Agreement and is providing the Services under such Services Order or Agreement will be deemed to be the Mimecast party entering into this DPA. All signatures provided on behalf of other Mimecast entities do not apply.

In the event of a conflict between this DPA and any other terms or conditions regarding the Processing of Personal Data contained in the Agreement (including any existing data processing addendum to the Agreement), this DPA shall control.

The terms herein apply to the Processing of Personal Data for the purposes set forth in the Agreement and this DPA.

Definitions. All capitalized terms used in this DPA and not otherwise defined shall have the same meaning attributed to them in the Agreement. The following definitions have the meanings set out below:

- **"Affiliate"** means an entity that controls, is directly or indirectly controlled by, or is under common control of the relevant party;
- **"Authorized Affiliate"** means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Mimecast, but has not signed its own Agreement with Mimecast and is not a "Customer" as defined under the Agreement;
- **"Applicable Law"** means one or more of the following data protection laws or regulations as applicable to the Processing of Personal Data by Mimecast under this DPA: (i) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"); (ii) the GDPR as incorporated into United Kingdom ("**UK**") law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 ("**UK GDPR**"); (iii) California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**"); (iv) the South Africa Protection of Personal Information Act ("**POPIA**"); (v) the Australia Privacy Act 1988 (No. 119 1988) (as amended), (vi) Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); and (vii) any law, regulation or order that implements the foregoing;
- **"Customer Data"** means data provided by Customer for processing via the Services including, without limitation, the contents of the files, emails or messages sent by or to a Permitted User;
- **"Data Subject"** means (i) "data subject" as defined under the GDPR, and (ii) "consumer" as defined under the CCPA;
- **"Data Subject Request"** refers to a request from a Data Subject in accordance the GDPR and/or the CCPA;
- **"EU Standard Contractual Clauses"** means the standard contractual clauses approved by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as applicable (referencing Module 2: Transfer Controller to Processor) and as may be amended or replaced by the European Commission from time-to-time;
- **"Instructions"** means (i) instructions from Customer as embodied in the Agreement, the applicable ordering documents and this DPA for those limited and specific purposes of providing the Service (the "Business Purpose" as defined under the CCPA), and (ii) those as may be additionally communicated in writing by Customer to Mimecast from time-to-time;
- **"Personal Data"** means (i) "personal data" as defined under the GDPR, and (ii) "personal information" as defined under CCPA, under the control of Customer and Processed by Mimecast in connection with the performance of the Services;
- **"Process", "Processed" or "Processing"** means "processing" as defined under the GDPR and the CCPA, the details of which are outlined on Schedule 1;
- **"Regulator"** means the data protection supervisory authority which has jurisdiction over Customer's Processing of Personal Data;
- **"Sale", "Sell" or "Selling"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data

with a Third Party, whether for monetary or other valuable considerations or for no consideration, for the Third Party's commercial purposes;

- **"Services"** means any and all services provided by Mimecast as identified in the Agreement and described further in an ordering document referencing the Agreement;
- **"Standard Contractual Clauses"** means the agreement pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of Personal Data to processors established in Third Countries approved by the EU Commission in Commission Decision 2010/87/EU, dated 5th February 2010;
- **"Third Country(ies)"** means countries outside of the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time-to-time;
- **"Third Party"** means any person (including companies, entities, organizations, etc.) that is not Customer or Mimecast;
- **"Third-Party Subcontractor"** means the third-party subcontractors listed in Schedule 2, as such list may be updated from time to time pursuant to Clause 8;
- **"Trust Center"** means the website created by Mimecast which includes relevant content referenced in this DPA and otherwise related to Applicable Law as well as Mimecast's operations and is found here: <https://www.mimecast.com/company/mimecast-trust-center/>;
- **"UK Addendum"** shall mean the International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018 as may be updated from time to time, currently found at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>.

Data Processing.

Mimecast shall only Process Personal Data on behalf of Customer in accordance with and for the purposes set out in the Instructions, which, for the avoidance of doubt and depending on the Services provided, may include Mimecast (i) providing the Customer with access to and use of the Services; and (ii) if applicable, improving and developing the Services, including but not limited to using Threat Data to train the Service's machine-learning algorithms, the output of which are anonymized and irreversible. Notwithstanding the foregoing, Processing may be required by Union or Member State law to which Mimecast is subject. In such a case, Mimecast shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

If the CCPA is applicable, Mimecast shall act as a "service provider" and certifies that it shall Process Customer Personal Data on behalf of Customer in accordance with and for the Business Purpose. Notwithstanding the foregoing, Mimecast may Process Customer Personal Data as may otherwise be permitted for service providers or under a comparable exemption from "Sale" under Applicable Law, as reasonably determined by Mimecast.

Each party shall comply with the obligations applicable to that party under Applicable Law.

Mimecast represents and warrants that:

- it shall promptly inform Customer if, in Mimecast's opinion: (i) Mimecast cannot comply with Applicable Law or (ii) Customer's Instructions violate Applicable Law, provided that Mimecast is not obliged to perform a comprehensive legal examination with respect to an Instruction of Customer;
- its personnel and Third-Party Subcontractors who are authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and
- Mimecast understands the restrictions placed on it under Section 2.2.

Customer represents and warrants that:

- its use of the Services and the Instructions provided do not contravene Applicable Law;

- it has complied and continues to comply with Applicable Law, in particular that it has obtained any necessary consents and/or given any necessary notices, and/or otherwise has the right to disclose Personal Data to Mimecast and enable the Processing set out in this DPA and as contemplated by the Agreement;
- it has assessed the requirements under Article 28 of the GDPR as they apply to Customer with regards to Personal Data and finds that the security measures referenced in Schedule 3 are adequate to meet those requirements;
- it will ensure compliance with and shall not in any way alter or diminish such security measures referenced in Schedule 3 to the extent applicable to Customer through its use of the Services; and
- where Processing hereunder includes, or may include, special categories of Personal Data, it has complied and continues to comply with requirements of Applicable Law to notify Data Subjects of the Processing and, where relevant, obtain any consents, or otherwise have the right to enable the Processing of the special categories of Personal Data.

Customer understands that Personal Data transferred to Mimecast is determined and controlled by Customer in its sole discretion. As such, Mimecast has no control over the volume, categories and sensitivity of Personal Data Processed through its Services by Customer or users. Mimecast shall implement and maintain the technical and organizational security measures specified in Schedule 3 hereto before Processing Customer's Personal Data and shall continue to comply with such technical and organizational security measures as a minimum standard of security during the term of the Agreement.

Notification of Data Breach. Mimecast shall notify Customer without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) of a declared breach of security which has led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer's Personal Data which affects the integrity, availability, or confidentiality of Customer's Personal Data ("Security Breach"). For the avoidance of doubt, Security Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems and no notice of the foregoing shall be required. In the event a Security Breach requires notification by Customer to Data Subjects or relevant Regulators, the parties agree to coordinate in good faith on developing the content of any public statements or required notices.

Audit and Inspection.

Mimecast shall provide reasonable assistance in response to inquiries from Customer or its Regulator relating to Mimecast's Processing of Customer's Personal Data.

Mimecast shall, upon written request from Customer, provide Customer with information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor pursuant to Mimecast's ISO27001 or similarly held industry certification.

In the event the information provided in accordance with Clause 4.2 above is insufficient to reasonably demonstrate compliance, Mimecast shall permit Customer to inspect or audit the technical and organizational measures of Mimecast for the purposes of monitoring compliance with Mimecast's obligations under this DPA no more than once per any twelve-month period. Any such inspection shall be:

- at Customer's expense;
- limited in scope to matters specific to Customer;
- agreed in advance between the parties in writing, including scope, duration, start date and Mimecast's then-current rates for professional services;
- conducted in a way which does not interfere with Mimecast's day-to-day business;
- during local business hours of Mimecast and, upon not less than twenty (20) business days advance written notice unless, in Customer's reasonable belief an identifiable, material non-conformance has arisen; and

- subject to the confidentiality obligations in the Agreement or, where a third-party auditor conducts the audit, such third-party auditor must be a professional bound by a duty of confidentiality or subject to a suitable non-disclosure agreement.

Any audit conducted under this Section shall not be conducted by a party who is a competitor of Mimecast.

Customer will provide Mimecast with copies of any audit reports generated in connection with any audit under this Section, unless prohibited by Applicable Law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

For the avoidance of doubt, the provisions of this Clause 4 shall also apply to the audit provisions of any Standard Contractual Clauses entered into in accordance with Clause 6 of this DPA.

Compliance, Co-operation, and Response.

Mimecast will provide reasonable assistance to Customer in complying with any Data Subject Requests or requests received by Customer from Regulators that occur in accordance with Applicable Law.

If Mimecast receives a Data Subject Request, and it is clear from the nature of the request without the need for any independent investigation that Customer is the applicable controller of Data Subject's Personal Data, Mimecast will refer the Data Subject to Customer, unless otherwise required by Applicable Law. In the event Mimecast is legally required to respond to the Data Subject, Customer will fully co-operate with Mimecast as appropriate. Customer agrees that provision of technical tools to enable Customer to take the necessary action to comply with such request/s shall be sufficient to discharge Mimecast's obligations of assistance hereunder.

Customer will reimburse all reasonable costs incurred by Mimecast as a result of reasonable assistance provided by Mimecast under this Clause 5.

Cross-Border Transfers. Customer acknowledges and agrees that Mimecast may, in the course of providing the Services, Process (or permit any Affiliate or Third-Party Subcontractor to Process) Customer's Personal Data in one or more Third Countries, provided that such Processing takes place in accordance with the requirements of Applicable Law. In such case, Mimecast shall, comply with (or procure that any Affiliate or Third-Party Subcontractor comply with) the data importer obligations in the Standard Contractual Clauses. Mimecast and its Affiliates have executed an Intercompany Agreement, a copy of which is available on the Trust Center, to provide for the adequate safeguards for the transfer of Personal Data among its Affiliates as such transfer may be necessary in order for Mimecast to fulfil its obligations under the Agreement. Customer hereby grants Mimecast a mandate to enter into the Standard Contractual Clauses with a Third-Party Subcontractor or Affiliate it appoints.

If, in fulfilling its obligations under the Agreement or pursuant to other lawful instructions from Customer, Personal Data is to be transferred from the European Economic Area, Switzerland and/or the UK (as applicable) by Customer to Mimecast in any Third Country, the parties agree to enter into and abide by the EU Standard Contractual Clauses and/or UK Addendum (as applicable), which are incorporated into this DPA as follows:

- Customer is the Data Exporter and Mimecast is the Data Importer (the foregoing shall apply with respect to Table 1 of the UK Addendum);
- Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated (the foregoing shall apply with respect to Table 1 of the UK Addendum);
- In Clause 9, the parties choose Option 2, 'General Written Authorisation', with a time period of 20 days (the foregoing shall apply with respect to Table 2 of the UK Addendum);
- The optional wording in Clause 11 shall be deemed not incorporated (the foregoing shall apply with respect to Table 2 of the UK Addendum);
- In Clause 17, the Data Exporter and Data Importer agree that the EU Standard Contractual Clauses shall be governed by the laws of Germany, and choose Option 1 to this effect (Part 2, Section 15(m) of the UK Addendum shall apply); In Clause 18, the Data Exporter and Data Importer agree that any disputes shall be resolved by the courts of Germany (Part 2, Section 15(n) of the UK Addendum shall apply);

- In accordance with Section 19 of the UK Addendum and Section 6.4 of this DPA, neither party may end the UK Addendum when the UK Addendum changes;
- Completed Annexes I, II and III of the EU Standard Contractual Clauses and Annexes 1B, II and III of Table 3 of the UK Addendum are included in Schedules 1-3 herein; and
- Notwithstanding the fact that the Standard Contractual Clauses are incorporated herein by reference without the Standard Contractual Clauses actually being signed by the parties, the parties agree that the execution of this DPA is deemed to constitute its execution of the Standard Contractual Clauses on behalf of the Data Exporter or Data Importer (as applicable), and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly.

The parties agree that the Standard Contractual Clauses shall cease to apply to the Processing of Personal Data if and to the extent that the relevant transfer of Personal Data ceases to be a “restricted transfer” by the relevant Regulator.

The provisions in this DPA shall be without prejudice to the parties’ ability to rely on any other legally valid international data transfer mechanism for the transfer of data out of the EEA and/or Switzerland.

The parties agree to enter into other standard contractual clauses approved under Applicable Law to the cross-border transfers of Personal Data for purposes of providing the Services.

The parties further agree that if any of the EU Standard Contractual Clauses or the UK Addendum are updated, replaced, or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Standard Contractual Clauses, as appropriate, or identify an alternative mechanism(s) to authorize the contemplated cross-border transfers.

Mimecast and its Affiliates have executed an Intercompany Agreement, a copy of which is available on the Trust Center (at <https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/mimecasts-intercompany-agreement/>), to provide for the adequate safeguards for the transfer of Personal Data among its Affiliates as such transfer may be necessary in order for Mimecast to fulfil its obligations under the Agreement.

Changes in Applicable Law. The parties agree to negotiate in good faith modifications to this DPA if changes are required for Mimecast to continue to Process Personal Data in compliance with Applicable Law, including but not limited to (i) the GDPR; (ii) the CCPA; (iii) any Standard Contractual Clauses; or (iv) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

Sub-Contracting.

Use of Third-Party Subcontractors. Customer hereby consents to the use of the Third-Party Subcontractors to perform Services. Subcontracting for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the principal obligation related to the processing of Personal Data pursuant to the Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Mimecast shall implement written agreements with all Third-Party Subcontractors that contain technical and organizational obligations on the Third-Party Subcontractors to safeguard the security and integrity of Personal Data that are no less protective than the obligations on Mimecast under this DPA in respect of the specific Services provided by the Third-Party Subcontractors.

Change to Third-Party Subcontractors. If Mimecast appoints a new Third-Party Subcontractor or intends to make any changes concerning the addition or replacement of the Third-Party Subcontractors, it shall provide Customer with at least 20 days written notice. For the purposes of this Clause 8.2, notice may be provided electronically, including but not limited to posting on the Mimecast administrative console of the Services, a notice on the Trust Center and/or in a e-newsletter sent to Customer (if Customer has subscribed to such e-newsletter via Mimecast’s online preference center). If Customer objects to the appointment or replacement of Third-Party Subcontractor in writing based on legitimate data protection grounds within ten (10) days after Mimecast’s advanced written notice of a new Third-Party Subcontractor, Mimecast, at its option may suggest a commercially reasonable change to Customer’s use of the Services so that the relevant Third-Party Subcontractor is not used in terms of the Service/s

procured. If Mimecast is unable to enact such change within a reasonable period of time, Customer may, upon not less than twenty (20) days' written notice from the date of notification by Mimecast, terminate the applicable Services Order with respect to those Services which cannot be provided without the use of the relevant Third-Party Subcontractor. If Customer does not provide a written objection within such ten (10) day period, Customer is deemed to have consented to such appointment or change in Third-Party Subcontractor. Termination of any ordering document under this Clause 8 shall entitle Customer to receive a pro-rata refund of any unused portion of the fees paid in advance. For the avoidance of doubt, termination under this Clause 8 shall not entitle Customer to any refund of fees paid for the period up to the effective date of termination.

Customer Data, Threat Data, Machine-Learning Data, and Aggregated Usage Data.

Customer Data. The parties acknowledge and agree that Mimecast has no ownership rights to Customer Data. In accordance with the Agreement and this DPA, Customer hereby grants to Mimecast a worldwide, irrevocable license to collect and process Customer Data, including certain Customer Data within Machine-Learning Data (as defined below), as well as Threat Data (as defined below) for the purposes of: (i) providing the Services; (ii) improving threat detection, analysis, awareness, and prevention; and/or (iii) improving and developing the Services.

Threat Data. As part of the Services, Mimecast processes certain data reasonably identified to be malicious, including, without limitation, data which may perpetuate data breaches, malware infections, cyberattacks or other threat activity (collectively, "**Threat Data**"). Mimecast processes Threat Data primarily through automated processes and may share limited Threat Data with third parties within the cybersecurity ecosystem for the purpose of improving threat detection, analysis and awareness. Threat Data is not Customer Data but may include Personal Data.

Machine-Learning Data. Through automated processes designed to develop and improve our machine learning algorithms within Services, Mimecast processes certain Customer Data and other data that describes and/or gives information about Customer Data, including but not limited to metadata, files, URLs, derived features and other data ("**Machine-Learning Data**"). We do not share Machine-Learning Data with Third Parties. Machine-Learning Data does not include full message content of Customer Data.

Aggregated Usage Data. Mimecast processes certain aggregated data derived from the Services, including usage data, such as utilization statistics, reports, logs and information regarding spam, viruses and/or other malware ("**Aggregated Usage Data**"). Mimecast owns all Aggregated Usage Data.

Confidentiality. The Confidentiality provisions in the Agreement shall apply equally to this DPA and where applicable, the Standard Contractual Clauses pursuant to Clause 6 therein.

Liability.

Limitations. The parties agree that Affiliates of Data Processor and/or Third-Party Subcontractors Processing Personal Data hereunder shall be bound by data protection obligations no less protective than the data protection obligations as specified in this DPA and any Standard Contractual Clauses entered into pursuant to Clause 6 herein. It is further agreed that the aggregate liability of the Affiliates, Third-Party Subcontractors and Data Processor under this DPA and any Standard Contractual Clauses entered into pursuant to this DPA, shall be no greater than the aggregate liability of Data Processor under the Agreement, to the extent permissible by Applicable Law. If Data Controller has contracted the Services through a managed services provider ("**MSP**"), Data Controller shall have no direct right of action against Data Processor with regards to the general provision of the Services and/or any instruction received from or access granted by the MSP, and all such claims should be brought against Data Controller's MSP. For the avoidance of doubt, the limitations of liability in the Agreement shall apply to this DPA and any Standard Contractual Clauses entered into in accordance with Clause 6 herein. Neither Data Controller nor any of its Authorized Affiliates shall be entitled to recover more than once in respect of the same claim under this DPA.

Satisfaction of claim. In the event of any claim by Customer against any Affiliate of Mimecast under the Standard Contractual Clauses, Customer shall accept payment from the Mimecast entity with whom Customer entered into the Agreement, on behalf of the relevant Affiliate of Mimecast in satisfaction of such claim.

Termination. Termination of this DPA shall be governed by the Agreement.

Consequences of Termination. Upon termination of this DPA in accordance with Clause 11, Mimecast shall, at Customer's request:

- delete all Personal Data Processed on behalf of Customer, unless applicable laws, regulations, subpoenas, or court orders require it to be retained; or
- assist Customer with the return to Customer of Personal Data and any copies thereof which it is Processing or has Processed upon behalf of Customer. Customer acknowledges and agrees that the nature of the Services mean that Customer may extract a copy of Personal Data at any time during the term of the Agreement and providing the tools to allow Customer to do so shall be sufficient to show Mimecast has complied with this Clause 12 (ii). If Customer requires Mimecast to extract Personal Data on its behalf, Customer must engage Mimecast in a professional services project, which shall be subject to additional fees; and
- in either case, cease Processing Personal Data on behalf of Customer, except as may otherwise be required in accordance with subparagraph (i) above.

Law and Jurisdiction. This DPA shall be governed by and construed in all respects in accordance with the governing law and jurisdiction provisions in the Agreement, provided that, in the event of a conflict between the Agreement and this DPA with regards to the Processing of Personal Data, this DPA shall control.

Parties to this DPA. The Section "HOW THIS DPA APPLIES" specifies which Mimecast entity is party to this DPA. Notwithstanding the signatures below of any other Mimecast entity, such other Mimecast entities are not a party to this DPA or the Standard Contractual Clauses.

This DPA may be executed in any number of counterparts, each of which is an original and all of which evidence the same agreement between the parties. For the avoidance of doubt, only the signature of the Mimecast entity that is providing the Services shall apply. All signatures on behalf of the other Mimecast entities shall have no force or effect.

CONTROL ENVIRONMENT

The control environment at Mimecast is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive board and operations management.

Integrity and Ethical Values

Mimecast is committed to conducting business ethically, responsibly, with integrity, and in compliance with applicable laws and regulations. Integrity and ethical values are important elements of Mimecast's control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

During induction, Mimecast personnel are required to read and accept the Code of Business Conduct and Ethics, which includes the entity's confidentiality and privacy practices. Management is accountable, and the Legal Team is responsible for monitoring personnel compliance with signing the Code of Business Conduct and Ethics. Mimecast monitors complaints and provides both internal and external reporting hotlines to enable anonymous reporting of known or suspected risk, malpractice, or wrongdoing. Disciplinary action outlined in the Code of Business Conduct and Ethics for non-compliance with policies are further enforced by regional HR practices in line with the local jurisdictions and the applicable laws, directives, statutes, acts, and other compliance requirements.

Specific control activities that Mimecast has implemented in this area are described below:

- Company policies include suspension and termination as potential sanctions for workforce members' misconduct.
- Management monitors personnel compliance with the code of business conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.
- Personnel are required to read and accept the code of business conduct and ethics policy, which includes the Company's confidentiality practices, at induction.
- Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.
- New personnel offered employment are subject to background checks.
- The Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.
- Employees are required to read and accept the Company's information security and acceptable use policies during induction.

Executive Board and Audit Committee Oversight

Mimecast's control consciousness is influenced significantly by its Executive Board. Attributes include the Executive Board and Audit Committee's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. The Executive Board oversees Mimecast's management activities, including the Enterprise Risk Management Executive Committee, which is responsible for governance and oversight of the Security Committee and Organizational Resilience Committee and includes the Company's owners and key executive members of management. Specific control activities that Mimecast has implemented in this area are described below:

- The executive board meets during the period and is consulted on all significant business and control-related matters. The board includes three subcommittees that are independent of management.
- The subcommittees have a documented charter that outlines its oversight responsibilities relative to internal control.

Organizational Structure and Assignment of Authority and Responsibility

Management has designed the organizational structure to provide quality service and accountability in support of Mimecast's mission. To achieve quality in performance, management personnel strive for continuous improvement in all that is done, plan and commit to accomplish targets, and are empowered to perform their duties. Mimecast's operations are highly specialized to adapt to industry changes and best practices. Mimecast has a centralized, flat management framework, which improves Mimecast's ability to quickly react to industry changes and user entity needs. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are available to personnel via the Company's intranet. Specific control activities that Mimecast has implemented in this area are described below:

- Management monitors personnel compliance with the code of business conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.
- The executive board has a documented charter that outlines its oversight responsibilities relative to internal control.
- The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.
- Roles and responsibilities are defined in written job descriptions.

Commitment to Competence

Mimecast's management philosophy and operating style is ultimately responsible for the system of internal controls. Virtually all employees have some role in controlling the organization. Some controls are established at the organization level, and management of the local business unit establishes others. Specific control activities that Mimecast has implemented in this area are described below:

- Roles and responsibilities are defined in written job descriptions.
- Employees are required to complete security training during induction. Security training includes training on the handling of sensitive data and developments in system security concepts and issues.
- All new hires are required to undergo a phishing e-mail program as a part of security awareness training.
- Employees are supported in their duties with access to the corporate learning management system (LMS) and policy repositories.

Accountability

Mimecast's HR policies and practices are clearly written and communicated, where appropriate. Many policies and procedures are available from the Company's intranet, including but not limited to hiring, training, disciplinary actions, and termination procedures. Specific control activities that Mimecast has implemented in this area are described below:

- Company policies include suspension and termination as potential sanctions for workforce members' misconduct
- Management monitors personnel compliance with the code of business conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.
- Personnel are required to read and accept the code of business conduct and ethics policy, which includes the Company's confidentiality practices, at induction.
- Roles and responsibilities are defined in written job descriptions.
- The Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.
- Employees are required to read and accept the Company's information security and acceptable use policies during induction.

RISK ASSESSMENT

Objective Setting

Management holds an annual company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives. Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. Management performs a risk assessment during the period to identify and analyze the business objective and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies.

Risk Identification and Analysis

Mimecast has established processes to identify and manage risks that could affect the Company's ability to provide secure, resilient, reliable services to its user entities. These include continually monitoring and evaluating potential risks through various means, including:

- Internal audits
- Internal vulnerability scans
- External ISO 27001, ISO 27701, and ISO 22301 auditing
- Enterprise Risk Management Committee meetings
- Security Committee meetings
- Organizational Resilience Committee and Weekly Business Continuity and Emergency Response meetings
- Internal and external third-party penetration tests and a variety of readiness assessments for attestations and certifications

Mimecast's risk assessment process is designed to identify and consider the implications of external and internal risk factors concurrent with establishing unit-wide objectives and plans. The likelihood of occurrence and of potential material, financial impact, including reputational risk, has been evaluated to enhance the reliability of management business processes. Risks are categorized as tolerable or requiring action and include the following considerations:

- Changes in the operating environment – a change in regulations may necessitate a revision of existing processing. Revisions of existing processing may create the need for additional or revised controls.
- New personnel – new personnel who are responsible for overseeing the IT controls may increase the risk that controls will not operate effectively.
- New or revamped information systems – new functions introduced into the system could affect user entities.
- Rapid growth – a rapid increase in the number of new user entities may affect the operating effectiveness of certain controls.
- New technology – the implementation of new application platforms or technology may operate so differently that it affects user entities.
- New business models, products, or activities – the diversion of resources to new activities from existing activities could affect certain controls.
- Corporate restructuring – a change in ownership or internal reorganization could affect reporting responsibilities or the resources available for services to user entities.
- Expanded foreign operations – the use of personnel in foreign locations to maintain programs used by domestic user entities may create difficulty in responding to changes in user requirements.
- System downtime – events could cause system downtime when the system fails to provide or perform its primary function for a period of time.
- Compromise of sensitive data – events that could cause the intentional or unintentional release of sensitive information to an untrusted environment.
- Government and regulatory changes – the implementation of relevant government and regulatory pronouncements could affect user entities.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments

- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Documented policies are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. A formal risk assessment is performed during the period that considers the potential for fraud and includes the evaluation of pressures, opportunities, and rationalization. Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures including fraudulent activity.

Risk Mitigation

The purpose of this continual risk assessment process is to conduct detailed evaluations of threats to security, availability, processing integrity, confidentiality, and privacy at Mimecast. This enables Mimecast to assess the potential liability, cost, likelihood, and repercussions of risks, threats, and vulnerabilities and to evaluate the effectiveness of the current controls, policies, and processes in minimizing, mitigating, or accepting the identified risks. Management's involvement in daily operations allows them to learn about risks related to information processing through direct, personal involvement with employees or outside parties and to incorporate consideration for these risks into the annual risk assessment process. Mimecast regularly reviews the risks that may threaten the achievement of the criteria for the security, availability, processing integrity, confidentiality, and privacy categories set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

TRUST SERVICES CRITERIA, CCM CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the

security, availability, processing integrity, confidentiality, and privacy categories and the requirements set forth in the CSA's CCM matrix version V4.0.3.

Selection and Development of Control Activities

The applicable trust services criteria, CCM criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria, CCM criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Mimecast's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria and CCM Criteria Not Applicable to the In-Scope System

The Trust Services criteria and CCM criteria presented below, are not applicable to the Mimecast Email Security system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted trust services criterion or CCM criteria. The following table presents the trust services criterion and CCM criteria that are not applicable for the Mimecast Email Security system at Mimecast. The not applicable trust services criteria are also described within Section 4.

Criteria #	Reason for Omitted Criteria
P1.1 DSP-08	Not Applicable – Providing notice to data subjects regarding privacy practices, including changes in the use of personal information, is the responsibility of the data controller and not Mimecast given its role as a data processor.
P2.1 DSP-11 DSP-12 DSP-13	Not Applicable – Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.
P3.2	Not Applicable – Obtaining consent and communicating the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.
P5.1	Not Applicable – Providing access to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.
P5.2	Not Applicable – Correcting, amending, or appending personal information is the responsibility of the data controller and not Mimecast given its role as a data processor.
P6.1 DSP-14	Not Applicable – Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Mimecast given its role as a data processor.
P6.7	Not Applicable – Providing an accounting to the data subject of the personal information held and disclosing a data subject's personal information is the responsibility of the data controller and not Mimecast given its role as a data processor.

INFORMATION AND COMMUNICATION SYSTEMS

Internal Communications

Mimecast has an Information Security Policy to help ensure that personnel understand their individual roles and responsibilities concerning information security. Responsibilities are also communicated through formal and informal training programs. Management is involved with day-to-day operations and can provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. Mimecast management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed. These methods include, but are not limited to, the following:

- Management has established defined roles and responsibilities to oversee the implementation of the information security policy.
- Roles and responsibilities are defined in written job descriptions.
- Employees are required to complete security training during induction. Security training includes training on the handling of sensitive data and developments in system security concepts and issues.
- All new hires are required to undergo a phishing e-mail program as a part of security awareness training.
- Employees are supported in their duties with access to the corporate LMS and policy repositories.
- System changes are communicated to authorized internal users via a ticketing system.
- System changes that result from incidents are communicated to customers through the customer-facing website. For major incidents, customers also receive an incident report.
- A formalized whistleblower policy is established, and an anonymous communication channel is in place for employees to report potential security issues or fraud concerns.

External Communications

Mimecast's system documents, including policies, procedures, security, training, and other relevant documentation, are available via the Company's intranet (The Knowledge, also known as "TK"), which is available to all Mimecast user entities. Mimecast uses preconfigured Slack channels to communicate security incidents, as well as system and facility availability issues, with relevant personnel. Mimecast communicates system significant availability and performance issues to user entities through one or more of the following channels, depending on the incident type and severity: short message service (SMS), e-mail, the Mimecast Administrative Console, Mimecast Service Monitor alerts, or through the Service Delivery department.

These methods include, but are not limited to, the following:

- Customers have the option to report operational failures, incidents, problems, concerns, and complaints. The process for customer reporting is described on the customer-facing website and in online system documentation.
- The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.
- Customers have access to an online knowledge base to support the configuration, usage monitoring, and access control of their administration console.
- Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.
- All customer-facing system changes are published on the customer-facing website.
- The Company maintains a documented Business Associate Agreement, which defines safeguards as a covered entity for Protected Health Information (PHI).

MONITORING

Security Monitoring

Mimecast's management performs monitoring activities to assess the quality of internal security controls over time and monitors activities throughout the year. If needed, corrective action is taken to address deviations from Company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

User Entity Communications Monitoring

Mimecast monitors user entity communications through the User Entity Success and Service Delivery business units. This information is provided to management, providing the ability to track, monitor, and assist in understanding user entity complaints or concerns, as well as to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor user entities' communications is an integral role in controlling the quality of the services it provides.

Management is proactive in responding to user entity concerns and complaints, and there is a high-level of inter-departmental communication about these events. These are handled immediately via an internal ticketing system and by personal contact by management staff. Major user entity-facing issues are immediately reported to the Executive Committee for discussion and approval of action.

Subservice Organization Monitoring

Colocation providers are monitored for their ability meet the Trust Services Criteria they provide to Mimecast through periodic review and verification of the provider's third-party certifications, attestations, and assessment reports through Mimecast audits, third-party audits, and other methods, as necessary.

Evaluating and Communicating Deficiencies

Deficiencies in management's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations and assessments of the internal control system and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes decisions for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria or the CCM criteria.

MIMECAST'S CONTROLS MAPPING TO CSA STAR V4.03 & PRIVACY

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
Audit and Assurance		
CCM: A&A-01	<i>Audit and Assurance Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	S226, S227, S2212, S521
CCM: A&A-02	<i>Independent Assessments</i> - Conduct independent audit and assurance assessments according to relevant standards at least annually.	S211, S213, S342
CCM: A&A-03	<i>Risk Based Planning Assessment</i> - Perform independent audit and assurance assessments according to risk-based plans and policies.	S211, S213, S342
CCM: A&A-04	<i>Data Security / Integrity</i> - Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	S234, S311, S312, S324, S325
CCM: A&A-05	<i>Audit Management Process</i> - Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	S226, S234, S311, S3121, S324
CCM: A&A-06	<i>Remediation</i> - Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	S211, S213, S311, S312, S324, S342
Application and Interface Security		
CCM: AIS-01	<i>Application and interface Security Policies and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	S222, S226, S523, S664
CCM: AIS-02	<i>Application Security Baseline Requirements</i> - Establish, document and maintain baseline requirements for securing different applications.	S523, S537, S538, S664
CCM: AIS-03	<i>Application Security Metrics</i> - Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	S212, S213, S216, S226, S732
CCM: AIS-04	<i>Secure Application Design and Development</i> - Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	S523, S537, S538, S732, I112
CCM: AIS-05	<i>Automated Application Security Testing</i> - Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	S226, S523, S537, S538, S612, S732, I112
CCM: AIS-06	<i>Automated Secure Application Deployment</i> - Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	S523, S536, S537, S538, S612, S732
CCM: AIS-07	<i>Application Vulnerability Remediation</i> - Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	S213, S342, S523, S536, S537, S538, S612, S732

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
Business Continuity Management and Operational Resilience		
CCM: BCR-01	<i>Business Continuity Management Policies and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	S222, S321, S322, A125, A128
CCM: BCR-02	<i>Risk Assessment and Impact Analysis</i> - Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	S222, S311, S312, S324
CCM: BCR-03	<i>Business Continuity Strategy</i> - Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	S222, S321, S322, A125, A128
CCM: BCR-04	<i>Business Continuity Planning</i> - Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	S222, S311, S321, S322
CCM: BCR-05	<i>Documentation</i> - Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and periodically.	S321, S322, A125, A126, A127, A128
CCM: BCR-06	<i>Business Continuity Exercises</i> - Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	S321, S322, S741
CCM: BCR-07	<i>Communication</i> - Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	S222, S321, S322, S741
CCM: BCR-08	<i>Backup</i> - Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	S321, S322, A126, A127, A128,
CCM: BCR-09	<i>Disaster Response Plan</i> - Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	S321, S322
CCM: BCR-10	<i>Response Plan Exercise</i> - Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities	S321, S322
CCM: BCR-11	<i>Equipment Redundancy</i> Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	S321, S322, A125, A126, A127, A128
Change Control and Configuration Management		
CCM: CCC-01	<i>Change Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	S53a, S226, S523, S536
CCM: CCC-02	<i>Quality Testing</i> - Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	S214, S229 S235, S523, S536, S537, S538, S818

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: CCC-03	<i>Change Management Technology</i> - Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	S229, S235, S523, S536, S537, S538, S818
CCM: CCC-04	<i>Unauthorized Change Protection</i> - Restrict the unauthorized addition, removal, update, and management of organization assets.	S229, S235, S523, S536, S537, S538, S818
CCM: CCC-05	<i>Change Agreements</i> - Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	S212, S537, S538
CCM: CCC-06	<i>Change Management Baseline</i> - Establish change management baselines for all relevant authorized changes on organization assets.	S523, S536, S818
CCM: CCC-07	<i>Detection of Baseline Deviation</i> - Implement detection measures with proactive notification in case of changes deviating from the established baseline.	S214, S537, S538, S664, S818, S6610
CCM: CCC-08	<i>Exception Management</i> - Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	S222, S523, S343, S732, S664, S818
CCM: CCC-09	<i>Change Restoration</i> - Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	S214, S537, S538
Cryptography, Encryption and Key Management		
CCM: CEK-01	<i>Encryption and Key Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	S6114, S619, S665, S726
CCM: CEK-02	<i>CEK Roles and Responsibilities</i> - Define and implement cryptographic, encryption and key management roles and responsibilities.	S6114, S611A
CCM: CEK-03	<i>Data Encryption</i> - Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	S6114, S619, S665, S671, S611A
CCM: CEK-04	<i>Encryption Algorithm</i> - Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	S6114, S616, S619, S665, S671, S611A
CCM: CEK-05	<i>Encryption Change Management</i> - Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	S6114, S523, S536, S537, S538, S523
CCM: CEK-06	<i>Encryption Change Cost Benefit Analysis</i> - Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis	S6114, S311, S312, S324
CCM: CEK-07	<i>Encryption Risk Management</i> - Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	S6114, S311, S312, S324
CCM: CEK-08	<i>CSC Key Management Capability</i> - CSPs must provide the capability for CSCs to manage their own data encryption keys.	S6114, S611A, S311, S312, S324

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: CEK-09	<i>Encryption and Key Management Audit</i> - Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	S6114, S611A, S311, S312, S324
CCM: CEK-10	<i>Key Generation</i> - Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	S619, S665
CCM: CEK-11	<i>Key Purpose</i> - Manage cryptographic secret and private keys that are provisioned for a unique purpose.	S6114, S611A
CCM: CEK-12	<i>Key Rotation</i> - Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	S6114, S611A
CCM: CEK-13	<i>Key Revocation</i> - Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	S6114, S611A
CCM: CEK-14	<i>Key Destruction</i> - Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	S6114, S611A
CCM: CEK-15	<i>Key Activation</i> - Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	S6114, S611A
CCM: CEK-16	<i>Key Suspension</i> - Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	S6114, S611A
CCM: CEK-17	<i>Key Deactivation</i> - Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	S6114, S611A, S523
CCM: CEK-18	<i>Key Archival</i> - Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	S6114, S611A
CCM: CEK-19	<i>Key Compromise</i> - Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	S6114, S611A
CCM: CEK-20	<i>Key Recovery</i> - Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	S6114, S611A, S523
CCM: CEK-21	<i>Key Inventory Management</i> - Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	S6114, S611A, S523

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
Data Center Security		
CCM- DCS-01	<i>Off-Site Equipment Disposal Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	S611, S651, C124
CCM: DCS-02	<i>Off-Site Transfer Authorization Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	S611, S651, C124
CCM: DCS-03	<i>Secure Area Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	S611, S651, C124
CCM: DCS-04	<i>Secure Media Transportation Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually	S611, S651, C124
CCM: DCS-05	<i>Assets Classification</i> - Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	S611, S651, C124
CCM: DCS-06	<i>Assets Cataloguing and Tracking</i> - Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	S611, S618
CCM: DCS-07	<i>Controlled Access Points</i> - Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas	S611, S618
CCM: DCS-08	<i>Equipment Identification</i> - Use equipment identification as a method for connection authentication.	S611, S618
CCM: DCS-09	<i>Secure Area Authorization</i> - Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Carve Out
CCM: DCS-10	<i>Surveillance System</i> - Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Carve Out
CCM: DCS-11	<i>Unauthorized Access Response Training</i> - Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Carve Out
CCM: DCS-12	<i>Cabling Security</i> - Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Carve Out
CCM: DCS-13	<i>Environmental Systems</i> - Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Carve Out

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: DCS-14	<i>Secure Utilities</i> - Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Carve Out
CCM: DCS-15	<i>Equipment Location</i> - Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Carve Out
Data Security and Privacy Lifecycle Management		
CCM: DSP-01	<i>Security and Privacy Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	S614, C115, C117, P435
CCM: DSP-02	<i>Secure Disposal</i> - Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	S651, C124, P435
CCM: DSP-03	<i>Data Inventory</i> - Create and maintain a data inventory, at least for any sensitive data and personal data.	S611, S726, C112
CCM: DSP-04	<i>Data Classification</i> - Classify data according to its type and sensitivity level.	S618, C115
CCM: DSP-05	<i>Data Flow Documentation</i> - Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	S611, S618, C112
CCM: DSP-06	<i>Data Ownership and Stewardship</i> - Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	S611, S618, S619, S665, C112
CCM: DSP-07	<i>Data Protection by Design and Default</i> - Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	I111, I112, I121, I122
CCM: DSP-08	<i>Data Privacy by Design and Default</i> - Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Not Applicable
CCM: DSP-09	<i>Data Protection Impact Assessment</i> - Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	P429
CCM: DSP-10	<i>Sensitive Data Transfer</i> - Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	S611, S618, S619, S665, C112
CCM: DSP-11	<i>Personal Data Access, Reversal, Rectification and Deletion</i> - Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations	Not Applicable
CCM: DSP-12	<i>Limitation of Purpose in Personal Data Processing</i> - Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Not Applicable

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: DSP-13	<i>Personal Data Sub-processing</i> - Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Not Applicable
CCM: DSP-14	<i>Disclosure of Data Sub-processors</i> - Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Not Applicable
CCM: DSP-15	<i>Limitation of Production Data Use</i> - Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	C114, S613, S615, A126
CCM: DSP-16	<i>Data Retention and Deletion</i> - Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	C112, C115, C117, C618, P423
CCM: DSP-17	<i>Sensitive Data Protection</i> - Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	S611, S618, S619, C112, S665
CCM: DSP-18	<i>Disclosure Notification</i> - The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	S614, S115, S619, S621, S665
CCM: DSP-19	<i>Data Location</i> - Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	S321, S322, A125, A126, A127, A128
Governance, Risk and Compliance		
CCM: GRC-01	<i>Governance Program Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	S131, S132, S133, S226
CCM: GRC-02	<i>Risk Management Program</i> - Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	S131, S132, S226, S311, S324
CCM: GRC-03	<i>Organizational Policy Reviews</i> - Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	S131, S132, S226
CCM: GRC-04	<i>Policy Exception Process</i> - Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	S111, S131, S132, S226
CCM: GRC-05	<i>Information Security Program</i> - Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	S131, S132, S226, S2213
CCM: GRC-06	<i>Governance Responsibility Mode</i> - Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs	S122, S131, S132, S226

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: GRC-07	<i>Information System Regulatory Mapping</i> - Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	S132, S216, S226, S232, S234, S324
CCM: GRC-08	<i>Special Interest Groups</i> - Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	S216
Human Resources		
CCM: HRS-01	<i>Background Screening Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	S142, S226
CCM: HRS-02	<i>Acceptable Use of Technology Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally owned or managed assets. Review and update the policies and procedures at least annually.	S226, S227, S2212
CCM: HRS-03	<i>Clean Desk Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	S132, S226, S227, S2212
CCM: HRS-04	<i>Remote and Home Working Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	S132, S226, S227, S2212
CCM: HRS-05	<i>Asset returns</i> - Establish and document procedures for the return of organization-owned assets by terminated employees.	S624, S651, C124
CCM: HRS-06	<i>Employment Termination</i> - Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	S226, S621, S624, S625
CCM: HRS-07	<i>Employment Agreement Process</i> - Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	S112, S113, S115
CCM: HRS-08	<i>Employment Agreement Consent</i> - The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies	S112, S113, S115
CCM: HRS-09	<i>Personnel Roles and Responsibilities</i> - Document and communicate roles and responsibilities of employees, as they relate to information assets and security	S112, S113, S115, S131 S133
CCM: HRS-10	<i>Non-Disclosure Agreements</i> - Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	S115, S232, S234, S325
CCM: HRS-11	<i>Security Awareness Training</i> - Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	S141, S228

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: HRS-12	<i>Personal and Sensitive Data Awareness and Training</i> - Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	S141, S228
CCM: HRS-13	<i>Compliance User Responsibility</i> - Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	S132, S133, S141, S226, S228
Identity and Access Management		
CCM: IAM-01	<i>Identity and Access Management Policy and Procedures</i> Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	S226, S524, S539
CCM: IAM-02	<i>Strong Password Policy and Procedures</i> - Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	S226, S524, S539
CCM: IAM-03	<i>Identity Inventory</i> - Manage, store, and review the information of system identities, and level of access.	S524, S539, S613, S615
CCM: IAM-04	<i>Separation of Duties</i> - Employ the separation of duties principle when implementing information system access.	S524, S539, S612, S613, S614, S615, S617, S621, S622, S623, S624, S6112
CCM: IAM-05	<i>Least Privilege</i> - Employ the least privilege principle when implementing information system access.	S524, S539, S612, S613, S614, S615, S617, S621, S622, S623, S624, S6112
CCM: IAM-06	<i>User Access Provisioning</i> - Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	S524, S622, S6112
CCM: IAM-07	<i>User Access Changes and Revocation</i> - De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	S621, S624, S625
CCM: IAM-08	<i>User Access Review</i> - Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	S621, S624, S625
CCM: IAM-09	<i>Segregation of Privileged Access Roles</i> - Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	S613, S614, S615
CCM: IAM-10	<i>Management of Privileged Access Roles</i> - Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period and implement procedures to prevent the culmination of segregated privileged access.	S613, S614, S615, S622, S6112
CCM: IAM-11	<i>CSCs Approval for Agreed Privileged Access Roles</i> - Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	S613, S614, S615, S621, S622

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: IAM-12	<i>Safeguard Logs Integrity</i> - Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures	S613, S614, S621, S663, S666
CCM: IAM-13	<i>Uniquely Identifiable Users</i> - Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	S613, S614, S615, S617, S621, S623
CCM: IAM-14	<i>Strong Authentication</i> - Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	S524, S539, S612, S613, S614, S615, S617, S621, S622, S623
CCM: IAM-15	<i>Passwords Management</i> - Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	S524, S539, S612, S613, S614, S615, S617
CCM: IAM-16	<i>Authorization Mechanisms</i> - Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	S524, S612, S613, S614, S615, S617, S621, S622, S623
Interoperability and Portability		
CCM: IPY-01	<i>Interoperability and Portability Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	S226, I111, I112
CCM: IPY-02	<i>Application Interface Availability</i> - Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	S232, I111, I112
CCM: IPY-03	<i>Secure Interoperability and Portability Management</i> - Implement cryptographically secure and standardized network protocols for the management, import and export of data.	S665, S6614, I111, I112
CCM: IPY-04	<i>Data Portability Contractual Obligations</i> - Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	S232, S651, C115, C124, I111, I112
Infrastructure and Virtualization Security		
CCM: IVS-01	<i>Infrastructure and Virtualization Security Policy and Procedures</i> Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	S226, S343, S664, S818

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: IVS-02	<i>Capacity and Resource Planning</i> - Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	S725, A111
CCM: IVS-03	<i>Network Security</i> - Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	S213, S226, S342, S662, S669, S665, S726
CCM: IVS-04	<i>OS Hardening and Base Controls</i> - Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	S226, S343, S664, S818
CCM: IVS-05	<i>Production and Non-Production Environments</i> - Separate production and non-production environments.	S226, S612
CCM: IVS-06	<i>Segmentation and Segregation</i> - Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	S664, S536, S523, S669, S662
CCM: IVS-07	<i>Migration to Cloud Environments</i> - Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	S226, S343, S612, S619, S664, S665, S818
CCM: IVS-08	<i>Network Architecture Documentation</i> - Identify and document high-risk environments.	S215, S226, S324, S616
CCM: IVS-09	<i>Network Defense</i> - Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	S662, S732
Logging and Monitoring		
CCM: LOG-01	<i>Logging and Monitoring Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	S226, S664, S818
CCM: LOG-02	<i>Audit Logs Protection</i> - Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	S212, S614, S663, S666, I133
CCM: LOG-03	<i>Security Monitoring and Alerting</i> - Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	S212, S231, S614, S663, S666, S732, I133
CCM: LOG-04	<i>Audit Logs Access and Accountability</i> - Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	S212, S231, S614, S663, S666, I133
CCM: LOG-05	<i>Audit Logs Monitoring and Response</i> - Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	S212, S231, S614, S663, S666, I133
CCM: LOG-06	<i>Clock Synchronization</i> - Use a reliable time source across all relevant information processing systems.	S727
CCM: LOG-07	<i>Logging Scope</i> - Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment	S212, S663

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: LOG-08	<i>Log Records</i> - Generate audit records containing relevant security information.	S212, S663
CCM: LOG-09	<i>Log Protection</i> - The information system protects audit records from unauthorized access, modification, and deletion.	S212, S231, S614, S663, S666, I133
CCM: LOG-10	<i>Encryption Monitoring and Reporting</i> - Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls	S212, S226, S663, S6114
CCM: LOG-11	<i>Transaction/Activity Logging</i> - Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	S212, S226, S663, S6114
CCM: LOG-12	<i>Access Control Logs</i> - Monitor and log physical access using an auditable access control system.	Carve Out
CCM: LOG-13	<i>Failures and Anomalies Reporting</i> - Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	S212, S614, S663, S732
Security Incident Management, e-Discovery, and Cloud Forensics		
CCM: SEF-01	<i>Security Incident Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	S222, S226, S723
CCM: SEF-02	<i>Service Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	S222, S226, S723
CCM: SEF-03	<i>Incident Response Plans</i> - Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.	S222, S226, S723
CCM: SEF-04	<i>Incident Response Testing</i> - Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	S222, S226, S741
CCM: SEF-05	<i>Incident Response Metrics</i> - Establish and monitor information security incident metrics.	S222, S723, S732, S742, S743
CCM: SEF-06	<i>Event Triage Processes</i> - Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	S222, S723, S732, S742, S743
CCM: SEF-07	<i>Security Breach Notification</i> - Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	S222, S723, S732, S742, S743
CCM: SEF-08	<i>Points of Contact Maintenance</i> - Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	S222, S226

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
Supply Chain Management, Transparency and Accountability		
CCM: STA-01	<i>SSRM Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually	S226, S234
CCM: STA-02	<i>SSRM Supply Chain</i> - Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	S226, S232, S234, S325
CCM: STA-03	<i>SSRM Guidance</i> - Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	S226, S232, S234, S325
CCM: STA-04	<i>SSRM Control Ownership</i> - Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	S226, S232, S234, S325
CCM: STA-05	<i>SSRM Documentation Review</i> - Review and validate SSRM documentation for all cloud services offerings the organization uses.	S226, S232, S234, S325
CCM: STA-06	<i>SSRM Control Implementation</i> - Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	S211, S226, S232, S234, S325
CCM: STA-07	<i>Supply Chain Inventory</i> - Develop and maintain an inventory of all supply chain relationships.	S226, S232, S234, S325, S611
CCM: STA-08	<i>Supply Chain Risk Management</i> - CSPs periodically review risk factors associated with all organizations within their supply chain.	S232, S234, S311, S324, S325
CCM: STA-09	<p><i>Primary Service and Contractual Agreement</i> - Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms:</p> <ul style="list-style-type: none"> • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy 	S226, S232, S234, S325
CCM: STA-10	<i>Supply Chain Agreement Review</i> - Review supply chain agreements between CSPs and CSCs at least annually.	S226, S232, S234, S325
CCM: STA-11	<i>Internal Compliance Testing</i> - Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	S226, S232, S234, S325
CCM: STA-12	<i>Supply Chain Service Agreement Compliance</i> - Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	S226, S232, S234, S325
CCM: STA-13	<i>Supply Chain Governance Review</i> - Periodically review the organization's supply chain partners' IT governance policies and procedures.	S226, S232, S234, S325

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: STA-14	<i>Supply Chain Data Security Assessment</i> - Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	S226, S232, S234, S325
Threat and Vulnerability Management		
CCM: TVM-01	<i>Threat and Vulnerability Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	S213, S226, S667, S6610
CCM: TVM-02	<i>Malware Protection Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	S213, S226, S667, S683, S684, S6610
CCM: TVM-03	<i>Vulnerability Remediation Schedule</i> - Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk	S213, S222, S226, S342, S667, S683, S684, S6610
CCM: TVM-04	<i>Detection Updates</i> - Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	S213, S222, S226, S342, S667, S683, S684, S6610
CCM: TVM-05	<i>External Library Vulnerabilities</i> - Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	S213, S222, S226, S342, S667, S683, S684, S6610
CCM: TVM-06	<i>Penetration Testing</i> - Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	S213, S342
CCM: TVM-07	<i>Vulnerability Identification</i> - Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	S213, S222, S226, S342, S667, S683, S684, S6610
CCM: TVM-08	<i>Vulnerability Prioritization</i> - Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	S213, S222, S226, S324, S342, S667, S683, S684, S6610
CCM: TVM-09	<i>Vulnerability Management Reporting</i> - Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	S213, S222, S226, S324, S342, S667, S683, S684, S6610
CCM: TVM-10	<i>Vulnerability Management Metrics</i> - Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	S213, S222, S226, S324, S342, S667, S683, S684, S6610
Universal Endpoint Management		
CCM: UEM-01	<i>Endpoint Devices Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	S226, S227, S2212
CCM: UEM-02	<i>Application and Service Approval</i> - Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	S226, S227, S343, S685, S2212
CCM: UEM-03	<i>Compatibility</i> - Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	S226, S227, S343, S662, S685, S2212

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
CCM: UEM-04	<i>Endpoint Inventory</i> - Maintain an inventory of all endpoints used to store and access company data.	S226, S343, S611, S662, S685
CCM: UEM-05	<i>Endpoint Management</i> - Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	S226, S343, S611, S662, S685
CCM: UEM-06	<i>Automatic Lock Screen</i> - Configure all relevant interactive-use endpoints to require an automatic lock screen.	S226, S6113
CCM: UEM-07	<i>Operating Systems</i> - Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	S214, S343, S537, S538, S662, S667, S685, S6610
CCM: UEM-08	<i>Storage Encryption</i> - Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	S226, S619, S671
CCM: UEM-09	<i>Anti-Malware Detection and Prevention</i> - Configure managed endpoints with anti-malware detection and prevention technology and services	S683, S684
CCM: UEM-10	<i>Software Firewall</i> - Configure managed endpoints with properly configured software firewalls.	S662, S666, S668, S669
CCM: UEM-11	<i>Data Loss Prevention</i> - Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment	C115, C116, C122, C125
CCM: UEM-12	<i>Remote Locate</i> - Enable remote geo-location capabilities for all managed mobile endpoints.	S611
CCM: UEM-13	<i>Remote Wipe</i> - Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	C122, C124, C125, C130
CCM: UEM-14	<i>Third-Party Endpoint Security Posture</i> - Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	S234, C325
Additional Criteria for Privacy		
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	Not Applicable
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	Not Applicable
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	C113, C115, S141, P111, P112, P813, P11a

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	Not Applicable
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	S115, S613, S614, S619, S621, S665
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	S618, C112, C115, C117, P423
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	S651, C124, P435
P5.1	The entity grants identified, and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	Not Applicable
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Not Applicable
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	Not Applicable
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	P611, P621
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	S222, P621, P662, P812, S732
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	P611, P652, S234, S325
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	S234, P652, P621, P611, P662
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	S222, S732, S742, P611, P621
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	Not Applicable
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	S619, S665, I121, I122, I133, I134

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	S222, S732, P611, P812, P814
Privacy Notice Commitments		
PNC1.0	Mimecast shall only Process Personal Data on behalf of Customer in accordance with and for the purposes set out in the Instructions, which, for the avoidance of doubt and depending on the Services provided, may include Mimecast (i) providing the Customer with access to and use of the Services; and (ii) if applicable, improving and developing the Services, including but not limited to using Threat Data to train the Service's machine-learning algorithms, the output of which are anonymized and irreversible. Notwithstanding the foregoing, Processing may be required by Union or Member State law to which Mimecast is subject. In such a case, Mimecast shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.	S141, S613, S614
PNC2.0	Mimecast shall notify Customer without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) of a declared breach of security which has led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer's Personal Data which affects the integrity, availability or confidentiality of Customer's Personal Data ("Security Breach"). For the avoidance of doubt, Security Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems and no notice of the foregoing shall be required. In the event a Security Breach requires notification by Customer to Data Subjects or relevant Regulators, the parties agree to coordinate in good faith on developing the content of any public statements or required notices.	S742, P611, P621, P662
PNC3.0	Customer hereby consents to the use of the Third-Party Subcontractors to perform Services. Subcontracting for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the principal obligation related to the processing of Personal Data pursuant to the Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Mimecast agrees that it has a written agreements in place with all Third-Party Subcontractors that contains obligations on the Third-Party Subcontractor that are no less onerous on the relevant Third-Party Subcontractor than the obligations on Mimecast under this DPA in respect of the specific Services provided by the Third-Party Subcontractor.	S234, S325, S619

Cloud Control Matrix Criteria No.	Criteria Common to Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories	Mimecast's Control No(s). (See Section 4)
PNC4.0	If Mimecast appoints a new Third-Party Subcontractor or intends to make any changes concerning the addition or replacement of the Third-Party Subcontractors, it shall provide Customer with reasonable advance written notice. For the purposes of this Clause 8.2, notice may be provided electronically, including but not limited to posting on the Mimecast administrative console of the Services, a notice on the Trust Center and/or in a e-newsletter sent to Customer (if Customer has subscribed to such e-newsletter via Mimecast's online preference center). If Customer objects to the appointment or replacement of Third-Party Subcontractor in writing based on legitimate data protection grounds within ten (10) days after Mimecast's advanced written notice of a new Third-Party Subcontractor.	S229, S234, S325
PNC5.0	Mimecast shall provide reasonable assistance in response to inquiries from Customer or its Regulator relating to Mimecast's Processing of Customer's Personal Data. Mimecast shall, upon written request from Customer, provide Customer with information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor.	S211, S313, S314
PNC6.0	Upon termination of this DPA in accordance with Clause 11, Mimecast shall, at Customer's request: delete all Personal Data Processed on behalf of Customer, unless applicable laws, regulations, subpoenas or court orders require it to be retained; or assist Customer with the return to Customer of Personal Data and any copies thereof which it is Processing or has Processed upon behalf of Customer. Customer acknowledges and agrees that the nature of the Services mean that Customer may extract a copy of Personal Data at any time during the term of the Agreement.	C125, P435

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Mimecast Email Security system provided by Mimecast. The scope of the testing was restricted to the Mimecast Email Security system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period November 1, 2022, to October 31, 2022.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria and CCM criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria and CCM criteria are presented in the “Complementary Controls at Subservice Organizations” sections, respectively, within Section 3.

AUDIT AND ASSURANCE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: A&A-01: <i>Audit and Assurance Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
A&A-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A&A-01.02	S227: Employees are required to read and accept the company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.
A&A-01.03	S2212: The Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.
A&A-01.04	S521: Policy and procedural documents for the implementation of security controls are documented and approved by the appropriate executive subcommittee at least annually.	Inspected the policy and procedural documents to determine that policy and procedural documents for the implementation of access management were documented and approved by the appropriate executive subcommittee during the period.	No exceptions noted.
CCM: A&A-02: Independent Assessments - Conduct independent audit and assurance assessments according to relevant standards at least annually.			
CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
A&A-02.01	S211: Internal audits are performed continuously and are based on specific compliance frameworks and international standards as determined by management. Controls are monitored and reported on the results of information security and privacy measures of performance.	Inquired of management regarding internal audits to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
		Inspected the evidence of the most recent internal audit to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A&A-02.02	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
A&A-02.03	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually, and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
CCM: A&A-03: Risk Based Planning Assessment - Perform independent audit and assurance assessments according to risk-based plans and policies.			
CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
A&A-03.01	S211: Internal audits are performed continuously and are based on specific compliance frameworks and international standards as determined by management. Controls are monitored and reported on the results of information security and privacy measures of performance.	Inquired of management regarding internal audits to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
		Inspected the evidence of the most recent internal audit to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
A&A-03.02	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A&A-03.03	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually, and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
CCM: A&A-04: <i>Requirements Compliance</i> - Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
A&A-04.01	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
A&A-04.02	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
A&A-04.03	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A&A-04.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
A&A-04.05	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: A&A-05: Audit Management Process - Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
A&A-05.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A&A-05.02	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
A&A-05.03	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
A&A-05.04	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
A&A-05.05	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: A&A-06: <i>Remediation</i> - Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
A&A-06.01	S211: Internal audits are performed continuously and are based on specific compliance frameworks and international standards as determined by management. Controls are monitored and reported on the results of information security and privacy measures of performance.	Inquired of management regarding internal audits to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
		Inspected the evidence of the most recent internal audit to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
A&A-06.02	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
A&A-06.03	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A&A-06.04	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
A&A-06.05	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
A&A-06.06	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually, and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.

[Intentionally Blank]

APPLICATION AND INTERFACE SECURITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: AIS-01: <i>Application and Interface Security Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
AIS-01.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
AIS-01.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
AIS-01.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related were in place to govern modification and maintenance of production systems.	No exceptions noted.
AIS-01.04	S664: The company has documented system hardening standards.	Inspected the system hardening procedures to determine that the company had documented system hardening procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: AIS-02: <i>Application Security Baseline Requirements</i> - Establish, document and maintain baseline requirements for securing different applications.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
AIS-02.01	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
AIS-02.02	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
AIS-02.03	S538: The company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
AIS-02.04	S664: The company has documented system hardening standards.	Inspected the system hardening procedures to determine that the company had documented system hardening procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: AIS-03: <i>Application Security Metrics</i> - Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.			
No mapping to SOC 2 TSCs.			
AIS-03.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
AIS-03.02	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
AIS-03.03	S216: The Company subscribes to industry security bulletins and e-mail alerts and uses them to monitor the impact of emerging technologies and security on the production systems.	Inspected the example security bulletin to determine that the Company subscribed to industry security bulletins and e-mail alerts and used them to monitor the impact of emerging technologies and security on the production systems.	No exceptions noted.
AIS-03.04	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
AIS-03.05	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: AIS-04: <i>Secure Application Design and Development</i> - Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
AIS-04.01	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
AIS-04.02	S537: The company infrastructure change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request was: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
AIS-04.03	S538: The company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the company infrastructure change management process required that each infrastructure change was: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
AIS-04.04	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
AIS-04.05	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.
CCM: AIS-05: <i>Automated Application Security Testing</i> - Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
AIS-05.01	S226: The company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
AIS-05.02	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
AIS-05.03	<p>S537: The company infrastructure change management process requires that software change requests are:</p> <ul style="list-style-type: none"> • Authorized • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	<p>Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request was:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
AIS-05.04	<p>S538: The company infrastructure change management process requires that infrastructure change requests are:</p> <ul style="list-style-type: none"> • Authorized • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	<p>Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the company infrastructure change management process required that each infrastructure change was:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
AIS-05.05	<p>S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.</p>	<p>Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
AIS-05.06	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
AIS-05.07	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.
CCM: AIS-06: <i>Automated Secure Application Deployment</i> - Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.			
No mapping to SOC 2 TSCs.			
AIS-06.01	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
AIS-06.02	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
AIS-06.03	<p>S537: The company software change management process requires that software change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	<p>Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
AIS-06.04	<p>S538: The company infrastructure change management process requires that infrastructure change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	<p>Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the company infrastructure change management process required that each infrastructure change is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
AIS-06.05	<p>S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.</p>	<p>Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.</p>	No exceptions noted.
AIS-06.06	<p>S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.</p>	<p>Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: AIS-07: <i>Application Vulnerability Remediation</i> - Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
AIS-07.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
AIS-07.02	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually, and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
AIS-07.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
AIS-07.04	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
AIS-07.05	<p>S537: The company software change management process requires that software change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	<p>Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
AIS-07.06	<p>S538: The company infrastructure change management process requires that infrastructure change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	<p>Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the company infrastructure change management process required that each infrastructure change is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
AIS-07.07	<p>S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.</p>	<p>Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.</p>	No exceptions noted.
AIS-07.08	<p>S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.</p>	<p>Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.</p>	No exceptions noted.

BUSINESS CONTINUITY MANAGEMENT & OPERATIONAL RESILIENCE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: BCR-01: <i>Business Continuity Management Policies and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
BCR-01.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
BCR-01.02	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-01.03	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-01.04	A125: The company uses a multi-location colocation strategy that is comprised of two data centers for each jurisdiction to permit the resumption of operations at other colocation facilities in the event of a total loss of one data center.	Inspected the evidence of redundant data centers for each jurisdiction to determine that the company used a multi-location strategy for its facilities to permit the resumption of operations at other Company data centers in the event of a total loss of one data center.	No exceptions noted.
BCR-01.05	A128: Formal procedures are documented which outline the process the company's staff follows to back up and recover customer data. The procedures are reviewed at least annually.	Inspected the backup and recovery procedures to determine that formal procedures were documented which outlined the process the company's staff follows to back up and recover customer data and the procedures were reviewed during the period.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: BCR-02: Risk Assessment and Impact Analysis - Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
BCR-02.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
BCR-02.02	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
BCR-02.03	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
BCR-02.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: BCR-03: <i>Business Continuity Strategy</i> - Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
BCR-03.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
BCR-03.02	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-03.03	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-03.04	A125: The company uses a multi-location colocation strategy that is comprised of two data centers for each jurisdiction to permit the resumption of operations at other colocation facilities in the event of a total loss of one data center.	Inspected the evidence of redundant data centers for each jurisdiction to determine that the company used a multi-location strategy for its facilities to permit the resumption of operations at other Company data centers in the event of a total loss of one data center.	No exceptions noted.
BCR-03.05	A128: Formal procedures are documented which outline the process the company's staff follows to back up and recover customer data. The procedures are reviewed at least annually.	Inspected the backup and recovery procedures to determine that formal procedures were documented which outlined the process the company's staff follows to back up and recover customer data and the procedures were reviewed during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: BCR-04: Business Continuity Planning - Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
BCR-04.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
BCR-04.02	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
BCR-04.03	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-04.04	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: BCR-05: Documentation - Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and periodically.			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
BCR-05.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-05.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-05.03	A125: The company uses a multi-location colocation strategy that is comprised of two data centers for each jurisdiction to permit the resumption of operations at other colocation facilities in the event of a total loss of one data center.	Inspected the evidence of redundant data centers for each jurisdiction to determine that the company used a multi-location strategy for its facilities to permit the resumption of operations at other Company data centers in the event of a total loss of one data center.	No exceptions noted.
BCR-05.04	A126: System configuration backups are performed using an automated system and replicated across the production environment to provide resiliency.	Inspected the backup configurations to determine that system configuration backups were performed using an automated system and replicated across the production environment to provide resiliency.	No exceptions noted.
BCR-05.05	A127: Archived customer data (e-mail) is replicated onto two separate servers within the same data center and a third copy is replicated to a third server hosted within a separate data center.	Inspected the replication configurations to determine that archived customer data (e-mail) was replicated onto two separate servers within the same data center and a third copy was replicated to a third server hosted within a separate data center.	No exceptions noted.
BCR-05.06	A128: Formal procedures are documented which outline the process the company's staff follows to back up and recover customer data. The procedures are reviewed at least annually.	Inspected the backup and recovery procedures to determine that formal procedures were documented which outlined the process the company's staff follows to back up and recover customer data and the procedures were reviewed during the period.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: BCR-06: <i>Business Continuity Exercises</i> - Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.			
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
BCR-06.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-06.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-06.03	S741: The incident response plan is tested at least annually and covers law enforcement requirements.	Inspected the incident response plan test to determine that the incident response plan was tested during the period and covered law enforcement requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: BCR-07: <i>Communication</i> - Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.			
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
BCR-07.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
BCR-07.02	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-07.03	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-07.04	S741: The incident response plan is tested at least annually and covers law enforcement requirements.	Inspected the incident response plan test to determine that the incident response plan was tested during the period and covered law enforcement requirements.	No exceptions noted.
CCM: BCR-08: <i>Backup</i> - Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
BCR-08.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
BCR-08.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-08.03	A126: System configuration backups are performed using an automated system and replicated across the production environment to provide resiliency.	Inspected the backup configurations to determine that system configuration backups were performed using an automated system and replicated across the production environment to provide resiliency.	No exceptions noted.
BCR-08.04	A127: Archived customer data (e-mail) is replicated onto two separate servers within the same data center and a third copy is replicated to a third server hosted within a separate data center.	Inspected the replication configurations to determine that archived customer data (e-mail) was replicated onto two separate servers within the same data center and a third copy was replicated to a third server hosted within a separate data center.	No exceptions noted.
BCR-08.05	A128: Formal procedures are documented which outline the process the company's staff follows to back up and recover customer data. The procedures are reviewed at least annually.	Inspected the backup and recovery procedures to determine that formal procedures were documented which outlined the process the company's staff follows to back up and recover customer data and the procedures were reviewed during the period.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.			
CCM: BCR-09: <i>Disaster Response Plan</i> - Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
BCR-09.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-09.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: BCR-10: Response Plan Exercise - Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.			
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
BCR-10.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-10.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: BCR-11: Equipment Redundancy - Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
BCR-11.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
BCR-11.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
BCR-11.03	A125: The company uses a multi-location colocation strategy that is comprised of two data centers for each jurisdiction to permit the resumption of operations at other colocation facilities in the event of a total loss of one data center.	Inspected the evidence of redundant data centers for each jurisdiction to determine that the company used a multi-location strategy for its facilities to permit the resumption of operations at other Company data centers in the event of a total loss of one data center.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
BCR-11.04	A126: System configuration backups are performed using an automated system and replicated across the production environment to provide resiliency.	Inspected the backup configurations to determine that system configuration backups were performed using an automated system and replicated across the production environment to provide resiliency.	No exceptions noted.
BCR-11.05	A127: Archived customer data (e-mail) is replicated onto two separate servers within the same data center and a third copy is replicated to a third server hosted within a separate data center.	Inspected the replication configurations to determine that archived customer data (e-mail) was replicated onto two separate servers within the same data center and a third copy was replicated to a third server hosted within a separate data center.	No exceptions noted.
BCR-11.06	A128: Formal procedures are documented which outline the process the company's staff follows to back up and recover customer data. The procedures are reviewed at least annually.	Inspected the backup and recovery procedures to determine that formal procedures were documented which outlined the process the company's staff follows to back up and recover customer data and the procedures were reviewed during the period.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		

CHANGE CONTROL AND CONFIGURATION MANAGEMENT

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CCC-01: <i>Change Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.			
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-01.01	S226: The company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
CCC-01.02	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCC-01.03	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.
CCC-01.04	S53a: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Inspected the change management process document to determine that the organization applied information security engineering principles in the specification, design, development, implementation, and modification of the information system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CCC-02: <i>Quality Testing</i> - Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-02.01	S214: A configuration management system is in place and monitors for configuration changes, reverts unauthorized changes back to the original state, and alerts administrators when changes occur.	Inspected the configuration tool configuration and example configuration change ticket to determine that a confirmation management system was in place and monitored for configuration changes, reverted unauthorized changes back to the original state, and alerted administrators when changes occurred.	No exceptions noted.
CCC-02.02	S229: Changes and notifications are communicated to subcontractors via e-mail and any supporting updates are logged within the ticketing systems.	Inspected the listing of changes and notifications for a sample of subcontractors during the period to determine that changes and notifications were communicated for each subcontractor sampled via e-mail and any supporting updates were logged within the ticketing system.	No exceptions noted.
CCC-02.03	S235: System changes that result from incidents are communicated to customers through the customer-facing website. For major incidents, customers also receive an incident report.	Observed the change tickets for a sample of incidents during the period to determine that each system change that resulted from incidents were communicated to customers through the customer-facing website and for major incidents, customers also received an incident report.	No exceptions noted.
CCC-02.04	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCC-02.05	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCC-02.06	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
CCC-02.07	S538: The Company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
CCC-02.08	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in Technical Operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in Technical Operations.	No exceptions noted.
CCM: CCC-03: <i>Change Management Technology</i> - Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-03.01	S229: Changes and notifications are communicated to subcontractors via e-mail and any supporting updates are logged within the ticketing systems.	Inspected the listing of changes and notifications for a sample of subcontractors during the period to determine that changes and notifications were communicated for each subcontractor sampled via e-mail and any supporting updates were logged within the ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCC-03.02	S235: System changes that result from incidents are communicated to customers through the customer-facing website. For major incidents, customers also receive an incident report.	Observed the change tickets for a sample of incidents during the period to determine that each system change that resulted from incidents were communicated to customers through the customer-facing website and for major incidents, customers also received an incident report.	No exceptions noted.
CCC-03.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCC-03.04	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.
CCC-03.05	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCC-03.06	S538: The Company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
CCC-03.07	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in technical operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in technical operations.	No exceptions noted.
CCM: CCC-04: <i>Unauthorized Change Protection</i> - Restrict the unauthorized addition, removal, update, and management of organization assets.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-04.01	S229: Changes and notifications are communicated to subcontractors via e-mail and any supporting updates are logged within the ticketing systems.	Inspected the listing of changes and notifications for a sample of subcontractors during the period to determine that changes and notifications were communicated for each subcontractor sampled via e-mail and any supporting updates were logged within the ticketing system.	No exceptions noted.
CCC-04.02	S235: System changes that result from incidents are communicated to customers through the customer-facing website. For major incidents, customers also receive an incident report.	Inspected the change tickets for a sample of incidents during the period to determine that system changes that resulted from incidents were communicated to customers through the customer-facing website and for major incidents, customers also received an incident report for each incident sampled.	No exceptions noted.
CCC-04.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCC-04.04	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.
CCC-04.05	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
CCC-04.06	S538: The Company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
CCC-04.07	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in technical operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in technical operations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CCC-05: <i>Change Agreements</i> - Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-05.01	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
CCC-05.02	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
CCC-05.03	S538: The Company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CCC-06: <i>Change Management Baseline</i> - Establish change management baselines for all relevant authorized changes on organization assets.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-06.01	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCC-06.02	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.
CCC-06.03	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in technical operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in technical operations.	No exceptions noted.
CCM: CCC-07: <i>Detection of Baseline Deviation</i> - Implement detection measures with proactive notification in case of changes deviating from the established baseline.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-07.01	S214: A configuration management system is in place and monitors for configuration changes, reverts unauthorized changes back to the original state, and alerts administrators when changes occur.	Inspected the configuration tool configuration and example configuration change ticket to determine that a confirmation management system was in place and monitored for configuration changes, reverted unauthorized changes back to the original state, and alerted administrators when changes occurred.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCC-07.02	<p>S537: The company software change management process requires that software change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	<p>Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
CCC-07.03	<p>S538: The Company infrastructure change management process requires that infrastructure change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	<p>Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
CCC-07.04	<p>S664: The Company has documented system hardening standards.</p>	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.
CCC-07.05	<p>S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in technical operations.</p>	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in technical operations.	No exceptions noted.
CCC-07.06	<p>S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.</p>	Inspected the patching configuration for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
<p>CCM: CCC-08: <i>Exception Management</i> - Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.</p>			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
C9.2 The entity assesses and manages risks associated with vendors and business partners.			
CCC-08.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
CCC-08.02	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCC-08.03	S343: The company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process to determine that the company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
CCC-08.04	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
CCC-08.05	S664: The Company has documented system hardening standards.	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCC-08.06	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in technical operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in technical operations.	No exceptions noted.
CCM: CCC-09: <i>Change Restoration</i> - Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CCC-09.01	S214: A configuration management system is in place and monitors for configuration changes, reverts unauthorized changes back to the original state, and alerts administrators when changes occur.	Inspected the configuration tool configuration and example configuration change ticket to determine that a confirmation management system was in place and monitored for configuration changes, reverted unauthorized changes back to the original state, and alerted administrators when changes occurred.	No exceptions noted.
CCC-09.02	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
CCC-09.03	S538: The company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.

CRYPTOGRAPHY, ENCRYPTION AND KEY MANAGEMENT

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CEK-01: <i>Encryption and Key Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CEK-01.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-01.02	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
CEK-01.03	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
CEK-01.04	S726: Media containing confidential information is required to be protected against unauthorized access, misuse, or corruption during transportation.	Inspected the data classification policy to determine that media containing confidential information was required to be protected against unauthorized access, misuse, or corruption during transportation.	No exceptions noted.
CCM: CEK-02: <i>CEK Roles and Responsibilities</i> - Define and implement cryptographic, encryption and key management roles and responsibilities.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-02.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-02.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-03: <i>Data Encryption</i> - Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CEK-03.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-03.02	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
CEK-03.03	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
CEK-03.04	S671: Internal storage for workstations and laptops is encrypted.	Inspected the employee workstation system configuration to determine that internal storage for workstations and laptops were encrypted.	No exceptions noted.
CEK-03.05	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-04: <i>Encryption Algorithm</i> - Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CEK-04.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-04.02	S616: Remote access by employees is permitted only through MFA over an encrypted VPN connection.	Inspected the VPN authentication configurations to determine that remote access by employees was permitted only through MFA over an encrypted VPN connection.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-04-03	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
CEK-04-04	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
CEK-04-05	S671: Internal storage for workstations and laptops is encrypted.	Inspected the employee workstation system configuration to determine that internal storage for workstations and laptops were encrypted.	No exceptions noted.
CEK-04-06	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-05: <i>Encryption Change Management</i> - Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.			
No mapping to SOC 2 TSCs.			
CEK-05-01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-05-02	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CEK-05-03	S536: A process exists to manage emergency changes. In order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocates additional resources to support the authorization and oversight of the emergency change management process.	Inspected the change management process document to determine that a process existed to manage emergency changes and in order to mitigate any additional risk associated with a compressed deployment timeline, the Company allocated additional resources to support the authorization and oversight of the emergency change management process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-05.04	S537: The company software change management process requires that software change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	Inspected the change request tickets for a sample of software changes during the period to determine that the company software change management process required that each software change request is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage Assessed for security implications	No exceptions noted.
CEK-05.05	S538: The Company infrastructure change management process requires that infrastructure change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
CEK-05.06	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCM: CEK-06: <i>Encryption Change Cost Benefit Analysis</i> - Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.			
No mapping to SOC 2 TSCs.			
CEK-06.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-06.02	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
CEK-06.03	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
CEK-06.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
CCM: CEK-07: Encryption Risk Management - Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-07.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-07.02	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-07.03	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
CEK-07.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
CCM: CEK-08: <i>CSC Key Management Capability</i> - CSPs must provide the capability for CSCs to manage their own data encryption keys.			
No mapping to SOC 2 TSCs.			
CEK-08.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-08.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CEK-08.03	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-08.04	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
CEK-08.05	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
CCM: CEK-09: <i>Encryption and Key Management Audit</i> - Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).			
No mapping to SOC 2 TSCs.			
CEK-09.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-09.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CEK-09.03	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-09.04	S312: The Company risk architecture consists of specialist risk committees for information security and business resilience, and each committee is chaired by an executive. The head of the ARC Committee is responsible for developing and overseeing the enterprise risk management program.	Inspected the enterprise risk management policy to determine that the company risk architecture consisted of specialist risk committees for information security and business resilience and each committee was chaired by an executive and the head of the ARC Committee was responsible for developing and overseeing the enterprise risk management program.	No exceptions noted.
CEK-09.05	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
CCM: CEK-10: Key Generation - Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.			
No mapping to SOC 2 TSCs.			
CEK-10.01	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
CEK-10.02	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
CCM: CEK-11: Key Purpose - Manage cryptographic secret and private keys that are provisioned for a unique purpose.			
No mapping to SOC 2 TSCs.			
CEK-11.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-11.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CEK-12: Key Rotation - Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-12.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-12.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-13: Key Revocation - Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-13.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-13.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-14: Key Destruction - Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-14.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-14.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: CEK-15: Key Activation - Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-15.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-15.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-16: Key Suspension - Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-16.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-16.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-17: Key Deactivation - Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.			
<i>No mapping to SOC 2 TSCs.</i>			
CEK-17.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-17.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-17.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCM: CEK-18: Key Archival - Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.			
No mapping to SOC 2 TSCs.			
CEK-18.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-18.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-19: Key Compromise - Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.			
No mapping to SOC 2 TSCs.			
CEK-19.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-19.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CCM: CEK-20: Key Recovery - Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.			
No mapping to SOC 2 TSCs.			
CEK-20.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CEK-20.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CEK-20.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.
CCM: CEK-21: Key Inventory Management - Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.			
No mapping to SOC 2 TSCs.			
CEK-21.01	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CEK-21.02	S611A: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with cryptographic policy.	Inspected the cryptographic control policy to determine that cryptographic keys were required for cryptography employed within the information system in accordance with the cryptography policy.	No exceptions noted.
CEK-21.03	S523: Formally documented change management procedures which include manage and adopt changes to cryptography, encryption, and key management-related are in place to govern the modification and maintenance of production systems.	Inspected the change management procedures to determine that formally documented change management procedures which included manage and adopt changes to encryption, and key management related are in place to govern modification and maintenance of production systems.	No exceptions noted.

DATA CENTER SECURITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DCS-01: <i>Off-Site Equipment Disposal Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.			
P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
P1.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.			
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
DCS-01.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-01.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of destroyed devices during the period to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DCS-01.03	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
CCM: DCS-02: <i>Off-Site Transfer Authorization Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
DCS-02.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-02.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of destroyed devices during the period to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
DCS-02.03	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DCS-03: <i>Secure Area Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.			
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
DCS-03.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-03.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of destroyed devices during the period to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
DCS-03.03	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DCS-04: <i>Secure Media Transportation Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
DCS-04.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-04.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of destroyed devices during the period to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
DCS-04.03	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
CCM: DCS-05: <i>Assets Classification</i> - Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
DCS-05.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DCS-05.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of destroyed devices during the period to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
DCS-05.03	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.			
CCM: DCS-06: <i>Assets Cataloguing and Tracking</i> - Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
DCS-06.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-06.03	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DCS-07: <i>Controlled Access Points</i> - Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.			
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
DCS-07.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-07.02	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.			
CCM: DCS-08: <i>Equipment Identification</i> - Use equipment identification as a method for connection authentication.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
DCS-08.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DCS-08.02	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DCS-09: Secure Area Authorization - Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.			
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
CCM: DCS-10: Surveillance System - Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.			
No mapping to SOC 2 TSCs.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
CCM: DCS-11: Unauthorized Access Response Training - Train datacenter personnel to respond to unauthorized ingress or egress attempts.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
CCM: DCS-12: Cabling Security - Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
CCM: DCS-13: Environmental Systems - Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DCS-14: Secure Utilities - Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.			
No mapping to SOC 2 TSCs.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		
CCM: DCS-15: Equipment Location - Keep business-critical equipment away from locations subject to high probability for environmental risk events.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.		

DATA SECURITY AND INFORMATION LIFECYCLE MANAGEMENT

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DSP-01: <i>Security and Privacy Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.			
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.			
P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.2 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
DSP-01.01	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-01.02	C115: The Company establishes written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the Company established written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
DSP-01.03	C117: The Company requires that the customer review and approve the Compliance Protect retention period once the product is enabled and before the retention period is enforced. The Compliance Protect retention period is visible in a read-only state to customers once approved	Inspected the data storage configuration during the period to determine that the Company required that the customer review and approve the compliance protect retention period once the product was enabled and before the retention period was enforced and the compliance protect retention period was visible in a read-only stat to each customer once approved.	No exceptions noted.
DSP-01.04	P435: The Company has implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	Inspected the user process for the identification and deletion of personal information to determine that the Company had implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	No exceptions noted.
CCM: DSP-02: <i>Secure Disposal</i> - Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
DSP-02.01	P435: The Company has implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	Inspected the user process for the identification and deletion of personal information to determine that the Company had implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-02.02	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
DSP-02.03	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
CCM: DSP-03: Data Inventory - Create and maintain a data inventory, at least for any sensitive data and personal data.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
DSP-03.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DSP-03.02	S726: Media containing confidential information is required to be protected against unauthorized access, misuse, or corruption during transportation.	Inspected the data classification policy to determine that media containing confidential information was required to be protected against unauthorized access, misuse, or corruption during transportation.	No exceptions noted.
DSP-03.03	C112: Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company.	Inspected the data classification policy and critical assets document to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
CCM: DSP-04: Data Classification - Classify data according to its type and sensitivity level.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
DSP-04.01	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-04.02	C115: The Company establishes written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the Company established written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
CCM: DSP-05: Data Flow Documentation - Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.			
<i>No mapping to SOC 2 TSCs.</i>			
DSP-05.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DSP-05.02	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
DSP-05.03	C112: Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company.	Inspected the data classification policy and critical assets document to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
CCM: DSP-06: Data Ownership and Stewardship - Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
P3.2 For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-06.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DSP-06.02	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
DSP-06.03	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
DSP-06.04	C112: Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company.	Inspected the data classification policy and critical assets document to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
DSP-06.05	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
CCM: DSP-07: <i>Data Protection by Design and Default</i> - Develop systems, products, and business practices based upon a principle of security by design and industry best practices.			
PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
DSP-07.01	I111: The Company uses open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Inspected the API documentation form from the customer-facing website to determine that the Company used open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-07.02	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.
DSP-07.03	I121: Customer-related field forms limit input to acceptable values for storage in the database.	Inspected the validation parameters and the validation process to determine that customer-related field forms limited input to acceptable values for storage in the database.	No exceptions noted.
DSP-07.04	I122: Customer-related field forms prevent submission if mandatory fields have not been completed.	Inspected the customer validation parameters and the validation process to determine that customer-related field forms prevented submission if mandatory fields had not been completed.	No exceptions noted.
CCM: DSP-08: <i>Data Privacy by Design and Default</i> - Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.			
P1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
	Not Applicable – Providing notice to data subjects regarding privacy practices, including changes in the use of personal information, is the responsibility of the data controller and not Mimecast given its role as a data processor.		
CCM: DSP-09: <i>Data Protection Impact Assessment</i> - Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
DSP-09.01	P429: A DPIA is in place to evaluate the risks upon the processing of personal data, according to any applicable laws, regulations, and industry best practices.	Inspected the most recent DPIA to determine that a DPIA was in place to evaluate the risks upon the processing of personal data, according to any applicable laws, regulations, and industry best practices.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DSP-10: Sensitive Data Transfer - Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
DSP-10.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DSP-10.02	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
DSP-10.03	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
DSP-10.04	C112: Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company.	Inspected the data classification policy and critical assets document to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
DSP-10.05	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
CCM: DSP-11: Personal Data Access, Reversal, Rectification and Deletion - Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
	Not Applicable – Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DSP-12: <i>Limitation of Purpose in Personal Data Processing</i> - Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity’s objectives related to privacy. The entity’s basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
	Not Applicable – Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.		
CCM: DSP-13: <i>Personal Data Sub-processing</i> - Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity’s objectives related to privacy. The entity’s basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
	Not Applicable – Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.		
CCM: DSP-14: <i>Disclosure of Data Sub-processors</i> - Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.			
P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity’s objectives related to privacy.			
	Not Applicable – Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Mimecast given its role as a data processor.		
CCM: DSP-15: <i>Limitation of Production Data Use</i> - Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.			
<i>No mapping to SOC 2 TSCs.</i>			
DSP-15.01	C114: The Company creates test data using a test data generator. Customer data is not used for development or QA testing.	Inspected the test generate scripts to determine that the Company created test data using a test data generator and customer data was not used for development or QA testing.	No exceptions noted.
DSP-15.02	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none">• Network• AdCon console• Operating system• Database• Firewall	Inspected the privileged access user listings to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none">• Network• AdCon console• Operating system• Database• Firewall	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-15.03	S615: Internal Identity and Access Management (IAM) controls ensure that only authorized personnel can access the high-value restricted information class (e.g., customer data).	Inspected the identity and access management (IAM) policies and procedures and the AuditMate dashboard to determine that IAM controls ensured that only authorized personnel can access the high-value information class.	No exceptions noted.
DSP-15.04	A126: System configuration backups are performed using an automated system and replicated across the production environment to provide resiliency.	Inspected the backup configurations to determine that system configuration backups were performed using an automated system and replicated across the production environment to provide resiliency.	No exceptions noted.
CCM: DSP-16: <i>Data Retention and Deletion</i> - Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.			
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.			
DSP-16.01	C115: The Company establishes written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the Company established written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
DSP-16.02	C117: The Company requires that the customer review and approve the Compliance Protect retention period once the product is enabled and before the retention period is enforced. The Compliance Protect retention period is visible in a read-only state to customers once approved	Inspected the data storage configuration during the period to determine that the Company required that the customer review and approve the compliance protect retention period once the product was enabled and before the retention period was enforced and the compliance protect retention period was visible in a read-only stat to each customer once approved.	No exceptions noted.
DSP-16.03	C112: Documents containing restricted customer information for business processes, systems, and third-party involvement are clearly identified as part of the classification systems of the Company	Inspected the data classification policy to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
DSP-16.04	C618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
DSP-16.05	P423: Security documentation is reviewed annually. In the event that improvements are required, previous version are retained for a period of at least six (6) years.	Inspected the security documentation and data storage configurations for a sample of customers to determine that security documentation was reviewed during the period and in the event the improvement were required, previous version were retained for a period of six years.	No exceptions noted.
CCM: DSP-17: <i>Sensitive Data Protection</i> - Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
P3.1 Personal information is collected consistent with the entity's objectives related to privacy.			
P3.2 For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.			
P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.			
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
P5.2 The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
P6.2 The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
P6.3 The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P6.4 The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
P6.5 The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.			
P6.6 The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
P6.7 The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
DSP-17.01	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
DSP-17.02	S618: A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
DSP-17.03	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
DSP-17.04	C112: Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company.	Inspected the data classification policy and critical assets document to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
DSP-17.05	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DSP-18: Disclosure Notification - The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.			
P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
DSP-18.01	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
DSP-18.02	S115: Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	Inspected the confidentiality and non-disclosure agreements for a sample of employees hired and current employees during the period to determine that confidentiality and non-disclosure agreements were established for each employee sampled that included clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	No exceptions noted.
DSP-18.03	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
DSP-18.04	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
DSP-18.05	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: DSP-19: Data Location - Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
DSP-19.01	S321: A documented business continuity and disaster recovery plan has been developed and is updated at least annually.	Inspected the business and disaster recovery plan to determine that a documented business continuity and disaster recovery plan had been developed and was updated during the period.	No exceptions noted.
DSP-19.02	S322: Business continuity and disaster recovery plan tests are performed at least annually. The process and the test results are reviewed for additional staff training purposes.	Inspected the most recent business continuity and disaster recovery test to determine that business and disaster recovery plan tests were performed during the period and the process, and the test results were reviewed for additional staff training purposes.	No exceptions noted.
DSP-19.03	A125: The Company uses a multi-location colocation strategy that is comprised of two data centers for each jurisdiction to permit the resumption of operations at other colocation facilities in the event of a total loss of one data center.	Inspected the evidence of redundant data centers for each jurisdiction to determine that the Company used a multi-location strategy for its facilities to permit the resumption of operations at other Company data centers in the event of a total loss of one data center.	No exceptions noted.
DSP-19.04	A126: System configuration backups are performed using an automated system and replicated across the production environment to provide resiliency.	Inspected the backup configurations to determine that system configuration backups were performed using an automated system and replicated across the production environment to provide resiliency.	No exceptions noted.
DSP-19.05	A127: Archived customer data (e-mail) is replicated onto two separate servers within the same data center and a third copy is replicated to a third server hosted within a separate data center.	Inspected the replication configurations to determine that archived customer data (e-mail) was replicated onto two separate servers within the same data center and a third copy was replicated to a third server hosted within a separate data center.	No exceptions noted.
DSP-19.06	A128: Formal procedures are documented which outline the process the Company's staff follows to back up and recover customer data. The procedures are reviewed at least annually.	Inspected the backup and recovery procedures to determine that formal procedures were documented which outlined the process the Company's staff follows to back up and recover customer data and the procedures were reviewed during the period.	No exceptions noted.
Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for implementing environmental protections within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media.			

GOVERNMENT, RISK AND COMPLIANCE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: GRC-01: Governance Program Policy and Procedures - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.			
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
GRC-01.01	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
GRC-01.02	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
GRC-01.03	S133: Roles and responsibilities are defined in written job descriptions.	Inspected the job descriptions for a sample of current employees during the period to determine that roles and responsibilities were defined in written job descriptions for each employee sampled.	No exceptions noted.
GRC-01.04	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
CCM: GRC-02: Risk Management Program - Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
GRC-02.01	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
GRC-02.02	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
GRC-02.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
GRC-02.04	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company has defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
GRC-02.05	S324: A master risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a master risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: GRC-03: <i>Organizational Policy Reviews</i> - Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
GRC-03.01	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
GRC-03.02	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
GRC-03.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
CCM: GRC-04: <i>Policy Exception Process</i> - Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
GRC-04.01	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
GRC-04.02	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
GRC-04.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
GRC-04.04	S111: Company policies include suspension and termination as potential sanctions for workforce members' misconduct.	Inspected the code of business conduct and ethics to determine that company policies included suspension and termination as potential sanctions for workforce members' misconduct.	No exceptions noted.
CCM: GRC-05: <i>Information Security Program</i> - Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.			
<i>No mapping to SOC 2 TSCs.</i>			
GRC-05.01	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
GRC-05.02	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
GRC-05.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
GRC-05.04	S2213: The Company maintains a comprehensive information security management system (ISMS).	Inspected the most recent ISMS report to determine that the Company maintained a comprehensive ISMS.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: GRC-06: <i>Governance Responsibility Mode</i> - Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.			
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
GRC-06.01	S122: The three subcommittees have a documented charter that outlines its oversight responsibilities relative to internal control.	Inspected the subcommittee charters to determine that the three subcommittees had a documented charter that outlined its oversight responsibilities relative to internal control.	No exceptions noted.
GRC-06.02	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
GRC-06.03	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
GRC-06.04	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
CCM: GRC-07: <i>Information System Regulatory Mapping</i> - Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.			
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
GRC-07.01	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
GRC-07.02	S216: The Company subscribes to industry security bulletins and e-mail alerts and uses them to monitor the impact of emerging technologies and security on the production systems.	Inspected the example security bulletin to determine that the Company subscribed to industry security bulletins and e-mail alerts and used them to monitor the impact of emerging technologies and security on the production systems.	No exceptions noted.
GRC-07.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
GRC-07.04	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
GRC-07.05	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
GRC-07.06	S324: A master risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a master risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: GRC-08: <i>Special Interest Groups</i> - Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.			
No mapping to SOC 2 TSCs.			
GRC-08.01	S216: The Company subscribes to industry security bulletins and e-mail alerts and uses them to monitor the impact of emerging technologies and security on the production systems.	Inspected the example security bulletin to determine that the Company subscribed to industry security bulletins and e-mail alerts and used them to monitor the impact of emerging technologies and security on the production systems.	No exceptions noted.

HUMAN RESOURCES

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-01: <i>Background Screening Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.			
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
HRS-01.01	S142: New personnel offered employment are subject to background checks.	Inspected the completed background checks for a sample of employees hired during the period to determine that new personnel offered employment were subject to background checks for each employee sampled.	No exceptions noted.
HRS-01.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-02: <i>Acceptable Use of Technology Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally owned or managed assets. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
HRS-02.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
HRS-02.02	S227: Employees are required to read and accept the Company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.
HRS-02.03	S2212: The Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.
CCM: HRS-03: <i>Clean Desk Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
HRS-03.01	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
HRS-03.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
HRS-03.03	S227: Employees are required to read and accept the Company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.
HRS-03.04	S2212: The Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.
CCM: HRS-04: <i>Remote and Home Working Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
HRS-04.01	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.
HRS-04.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
HRS-04.03	S227: Employees are required to read and accept the Company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
HRS-04.04	S2212: The Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.
CCM: HRS-05: <i>Asset returns</i> - Establish and document procedures for the return of organization-owned assets by terminated employees.			
<i>No mapping to SOC 2 TSCs.</i>			
HRS-05.01	S624: When a user is terminated, all associated logical and physical access accounts are disabled and all Company assets in their possession are returned.	Inspected the termination tickets for a sample of employees terminated during the period to determine that when a user is terminated, all associated logical and physical access accounts were disabled and all Company assets in their possession were returned for each employee sampled.	No exceptions noted.
HRS-05.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction for a sample of destroyed devices during the period to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
HRS-05.03	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-06: <i>Employment Termination</i> - Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
HRS-06.01	S226: The company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
HRS-06.02	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
HRS-06.03	S624: When a user is terminated, all associated logical and physical access accounts are disabled and all Company assets in their possession are returned.	Inspected the termination tickets for a sample of employees terminated during the period to determine that when a user is terminated, all associated logical and physical access accounts were disabled and all Company assets in their possession were returned for each employee sampled.	No exceptions noted.
HRS-06.04	S625: An automated script runs multiple times a day that compares corporate AD accounts to the production environment LDAP directory. The script disables any account in the production environment LDAP directory if the corporate AD account is disabled, and alerts are sent to management for any account changes.	Inspected the script configurations and alert configurations to determine that an automated script ran multiple times a day that compared corporate AD accounts to the production environment LDAP directory and the script disabled any account in the production environment LDAP directory if the corporate AD account was disabled, and alerts were sent to management for any account changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-07: <i>Employment Agreement Process</i> - Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
SCC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
HRS-07.01	S112: Management monitors personnel compliance with the code of business conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.	Inspected the code of business conduct and ethics portal dashboard to determine that management monitored personnel compliance with the code of conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.	No exceptions noted.
HRS-07.02	S113: Personnel are required to read and accept the code of business conduct and ethics policy, which includes the Company's confidentiality practices, at induction.	Inspected the code of business conduct and ethics policy acknowledgements for a sample of employees hired during the period to determine that personnel were required to read and accept the code of business conduct and ethics policy, which included the Company's confidentiality practices, at induction for each employee sampled.	No exceptions noted.
HRS-07.03	S115: Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	Inspected the confidentiality and non-disclosure agreements for a sample of employees hired and current employees during the period to determine that confidentiality and non-disclosure agreements were established for each employee sampled that included clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-08: <i>Employment Agreement Consent</i> – The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
HRS-08.01	S112: Management monitors personnel compliance with the code of business conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.	Inspected the code of business conduct and ethics portal dashboard to determine that management monitored personnel compliance with the code of conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.	No exceptions noted.
HRS-08.02	S113: Personnel are required to read and accept the code of business conduct and ethics policy, which includes the Company's confidentiality practices, at induction.	Inspected the code of business conduct and ethics policy acknowledgements for a sample of employees hired during the period to determine that personnel were required to read and accept the code of business conduct and ethics policy, which included the Company's confidentiality practices, at induction for each employee sampled.	No exceptions noted.
HRS-08.03	S115: Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	Inspected the confidentiality and non-disclosure agreements for a sample of employees hired and current employees during the period to determine that confidentiality and non-disclosure agreements were established for each employee sampled that included clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-09: Personnel Roles and Responsibilities - Document and communicate roles and responsibilities of employees, as they relate to information assets and security.			
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
HRS-09.01	S112: Management monitors personnel compliance with the code of business conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.	Inspected the code of business conduct and ethics portal dashboard to determine that management monitored personnel compliance with the code of conduct and ethics through the monitoring of customer and employee complaints and the use of an administered ethics hotline.	No exceptions noted.
HRS-09.02	S113: Personnel are required to read and accept the code of business conduct and ethics policy, which includes the Company's confidentiality practices, at induction.	Inspected the code of business conduct and ethics policy acknowledgements for a sample of employees hired during the period to determine that personnel were required to read and accept the code of business conduct and ethics policy, which included the Company's confidentiality practices, at induction for each employee sampled.	No exceptions noted.
HRS-09.03	S115: Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	Inspected the confidentiality and non-disclosure agreements for a sample of employees hired and current employees during the period to determine that confidentiality and non-disclosure agreements were established for each employee sampled that included clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	No exceptions noted.
HRS-09.04	S131: The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organizational chart to determine that the Company had an organization chart that defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
HRS-09.05	S133: Roles and responsibilities are defined in written job descriptions.	Inspected the job descriptions for a sample of current employees during the period to determine that roles and responsibilities were defined in written job descriptions for each employee sampled.	No exceptions noted.
CCM: HRS-10: Non-Disclosure Agreements - Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
P6.4 The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
HRS-10.01	S115: Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	Inspected the confidentiality and non-disclosure agreements for a sample of employees hired and current employees during the period to determine that confidentiality and non-disclosure agreements were established for each employee sampled that included clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	No exceptions noted.
HRS-10.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
HR-10.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
HR-10.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: HRS-11: Security Awareness Training - Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
HRS-11.01	S141: Employees are required to complete security training during induction. Security training includes training on the handling of sensitive data and developments in system security concepts and issues.	Inspected the security awareness training records for a sample of employees hired during the period to determine that employees were required to complete security training during induction and security training included training on the handling of sensitive data and developments in system security concepts and issues for each employee sampled.	No exceptions noted.
HRS-11.02	S228: Employees are supported in their duties with access to the corporate LMS and policy repositories.	Inspected the learning management system to determine that employees were supported in their duties with access to the corporate LMS and policy repositories.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: HRS-12: <i>Personal and Sensitive Data Awareness and Training</i> - Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
HRS-12.01	S141: Employees are required to complete security training during induction. Security training includes training on the handling of sensitive data and developments in system security concepts and issues.	Inspected the security awareness training records for a sample of employees hired during the period to determine that employees were required to complete security training during induction and security training included training on the handling of sensitive data and developments in system security concepts and issues for each employee sampled.	No exceptions noted.
HRS-12.02	S228: Employees are supported in their duties with access to the corporate LMS and policy repositories.	Inspected the learning management system to determine that employees were supported in their duties with access to the corporate LMS and policy repositories.	No exceptions noted.
CCM: HRS-13: <i>Compliance User Responsibility</i> - Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.			
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
HRS-13.01	S133: Roles and responsibilities are defined in written job descriptions.	Inspected the job descriptions for a sample of current employees during the period to determine that roles and responsibilities were defined in written job descriptions for each employee sampled.	No exceptions noted.
HRS-13.02	S132: Management has established defined roles and responsibilities to oversee the implementation of the information security policy.	Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the information security policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
HRS-13.03	S141: Employees are required to complete security training during induction. Security training includes training on the handling of sensitive data and developments in system security concepts and issues.	Inspected the security awareness training records for a sample of employees hired during the period to determine that employees were required to complete security training during induction and security training included training on the handling of sensitive data and developments in system security concepts and issues for each employee sampled.	No exceptions noted.
HRS-13.04	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
HRS-13.05	S228: Employees are supported in their duties with access to the corporate LMS and policy repositories.	Inspected the learning management system to determine that employees were supported in their duties with access to the corporate LMS and policy repositories.	No exceptions noted.

IDENTITY AND ACCESS MANAGEMENT

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-01: <i>Identity and Access Management Policy and Procedures</i> - Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IAM-01.02	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-01.03	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-02: Strong Password Policy and Procedures - Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.			
No mapping to SOC 2 TSCs.			
IAM-02.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IAM-02.02	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-02.03	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.
CCM: IAM-03: Identity Inventory - Manage, store, and review the information of system identities, and level of access.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-03.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-03.02	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-03.03	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-03.04	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
CCM: IAM-04: Separation of Duties - Employ the separation of duties principle when implementing information system access.			
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-04.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-04.02	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.
IAM-04.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IAM-04.04	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-04.05	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
IAM-04.06	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-04.07	S617: Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	Inspected the password configurations for a sample of in-scope systems during the period to determine that passwords for each in-scope system was configured according to the Company's policy and Company policy required the following (unless there was a system limitations): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	No exceptions noted.
IAM-04.08	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-04.09	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-04.10	S623: Privileged customer administrator accounts are created in the application based on a written authorization request from the designated customer point of contact.	Inspected the written authorization requests for a sample of customer administrator accounts provisioned during the period to determine that privileged customer administrator accounts were created in the application based on a written authorization request from the designated customer point of contact for each customer administrator account sampled.	No exceptions noted.
IAM-04.11	S624: When a user is terminated, all associated logical and physical access accounts are disabled and all Company assets in their possession are returned.	Inspected the termination tickets for a sample of employees terminated during the period to determine that when a user is terminated, all associated logical and physical access accounts were disabled and all Company assets in their possession were returned for each employee sampled.	No exceptions noted.
IAM-04.12	S6112: Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request forms for a sample of users during the period to determine that access to in-scope systems components required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.
CCM: IAM-05: <i>Least Privilege</i> - Employ the least privilege principle when implementing information system access.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-05.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-05.02	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-05.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IAM-05.04	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database Firewall 	No exceptions noted.
IAM-05.05	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-05.06	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-05.07	S617: Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	Inspected the password configurations for a sample of in-scope systems during the period to determine that passwords for each in-scope system was configured according to the Company's policy and Company policy required the following (unless there was a system limitations): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	No exceptions noted.
IAM-05.08	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-05.09	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
IAM-05.10	S623: Privileged customer administrator accounts are created in the application based on a written authorization request from the designated customer point of contact.	Inspected the written authorization requests for a sample of customer administrator accounts provisioned during the period to determine that privileged customer administrator accounts were created in the application based on a written authorization request from the designated customer point of contact for each customer administrator account sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-05.11	S624: When a user is terminated, all associated logical and physical access accounts are disabled and all Company assets in their possession are returned.	Inspected the termination tickets for a sample of employees terminated during the period to determine that when a user is terminated, all associated logical and physical access accounts were disabled and all Company assets in their possession were returned for each employee sampled.	No exceptions noted.
IAM-05.12	S6112: Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request forms for a sample of users during the period to determine that access to in-scope systems components required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.
CCM: IAM-06: User Access Provisioning - Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
IAM-06.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-06.02	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
IAM-06.03	S6112: Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request forms for a sample of users during the period to determine that access to in-scope systems components required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-07: User Access Changes and Revocation - De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-07.01	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-07.02	S624: When a user is terminated, all associated logical and physical access accounts are disabled and all Company assets in their possession are returned.	Inspected the termination tickets for a sample of employees terminated during the period to determine that when a user is terminated, all associated logical and physical access accounts were disabled and all Company assets in their possession were returned for each employee sampled.	No exceptions noted.
IAM-07.03	S625: An automated script runs multiple times a day that compares corporate AD accounts to the production environment LDAP directory. The script disables any account in the production environment LDAP directory if the corporate AD account is disabled, and alerts are sent to management for any account changes.	Inspected the script configurations and alert configurations to determine that an automated script ran multiple times a day that compared corporate AD accounts to the production environment LDAP directory and the script disabled any account in the production environment LDAP directory if the corporate AD account was disabled, and alerts were sent to management for any account changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-08: <i>User Access Review</i> - Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-08.01	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-08.02	S624: When a user is terminated, all associated logical and physical access accounts are disabled and all Company assets in their possession are returned.	Inspected the termination tickets for a sample of employees terminated during the period to determine that when a user is terminated, all associated logical and physical access accounts were disabled and all Company assets in their possession were returned for each employee sampled.	No exceptions noted.
IAM-08.03	S625: An automated script runs multiple times a day that compares corporate AD accounts to the production environment LDAP directory. The script disables any account in the production environment LDAP directory if the corporate AD account is disabled, and alerts are sent to management for any account changes.	Inspected the script configurations and alert configurations to determine that an automated script ran multiple times a day that compared corporate AD accounts to the production environment LDAP directory and the script disabled any account in the production environment LDAP directory if the corporate AD account was disabled, and alerts were sent to management for any account changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-09: <i>Segregation of Privileged Access Roles</i> - Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-09.01	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-09.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-09.03	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
CCM: IAM-10: Management of Privileged Access Roles - Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period and implement procedures to prevent the culmination of segregated privileged access.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-10.01	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-10.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
IAM-10.03	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-10.04	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
IAM-10.05	S6112: Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request forms for a sample of users during the period to determine that access to in-scope systems components required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-11: CSCs Approval for Agreed Privileged Access Roles - Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
IAM-11.01	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-11.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-11.03	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-11.04	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-11.05	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
CCM: IAM-12: Safeguard Logs Integrity - Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.			
No mapping to SOC 2 TSCs.			
IAM-12.01	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-12.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
IAM-12.03	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-12.04	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
IAM-12.05	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.
CCM: IAM-13: Uniquely Identifiable Users - Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.			
SOC 2 CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
IAM-13.01	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need:</p> <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-13.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
IAM-13.03	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-13.04	<p>S617: Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation):</p> <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	<p>Inspected the password configurations for a sample of in-scope systems during the period to determine that passwords for each in-scope system was configured according to the Company's policy and Company policy required the following (unless there was a system limitations):</p> <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-13.05	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-13.06	S623: Privileged customer administrator accounts are created in the application based on a written authorization request from the designated customer point of contact.	Inspected the written authorization requests for a sample of customer administrator accounts provisioned during the period to determine that privileged customer administrator accounts were created in the application based on a written authorization request from the designated customer point of contact for each customer administrator account sampled.	No exceptions noted.
CCM: IAM-14: Strong Authentication - Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
IAM-14.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-14.02	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IMA-14.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IAM-14.04	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database Firewall	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-14.05	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-14.06	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-14.07	S617: Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) Password expiration enabled	Inspected the password configurations for a sample of in-scope systems during the period to determine that passwords for each in-scope system was configured according to the Company's policy and Company policy required the following (unless there was a system limitations): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) Password expiration enabled	No exceptions noted.
IAM-14.08	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-14.09	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
IAM-14.10	S623: Privileged customer administrator accounts are created in the application based on a written authorization request from the designated customer point of contact.	Inspected the written authorization requests for a sample of customer administrator accounts provisioned during the period to determine that privileged customer administrator accounts were created in the application based on a written authorization request from the designated customer point of contact for each customer administrator account sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IAM-15: Passwords Management - Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
IAM-15.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-15.02	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.
IAM-15.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IAM-15.04	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need:</p> <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-15.05	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
IAM-15.06	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-15.07	<p>S617: Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation):</p> <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) • Password expiration enabled 	<p>Inspected the password configurations for a sample of in-scope systems during the period to determine that passwords for each in-scope system was configured according to the Company's policy and Company policy required the following (unless there was a system limitations):</p> <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) <p>Password expiration enabled</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-15.08	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-15.09	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
IAM-15.10	S623: Privileged customer administrator accounts are created in the application based on a written authorization request from the designated customer point of contact.	Inspected the written authorization requests for a sample of customer administrator accounts provisioned during the period to determine that privileged customer administrator accounts were created in the application based on a written authorization request from the designated customer point of contact for each customer administrator account sampled.	No exceptions noted.
CCM: IAM-16: Authorization Mechanisms - Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives			
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
IAM-16.01	S524: The Company has a documented logical access process that defines segregation of duties where appropriate.	Inspected the identity and access management process document to determine that the Company had a documented logical access process that define segregation of duties where appropriate.	No exceptions noted.
IAM-16.02	S539: Policies and procedures are established for permissible storage and access of identities used for authentication to ensure that identities are only accessible based on the rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Inspected the identity and access management policies and procedures to determine that policies and procedures were established for permissible storage and access of identities used for authentication to ensure that identities were only accessible based on the rules of least privilege and replication limitations only to users explicitly defined as business necessary.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-16.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IAM-16.04	S613: Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of management to determine that privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
IAM-16.05	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IAM-16.06	S615: Internal IAM controls ensure that only authorized personnel can access high value 'restricted' information class and includes requirements for limiting the time period of privileged access roles and rights, is defined.	Inspected the IAM policies and user listing for a sample of in-scope systems during the period to determine that internal IAM controls ensured that only authorized personnel can access the high-value information class and includes requirements for limiting the time period of privileged access roles and rights, was defined for each of the in-scope systems sampled.	No exceptions noted.
IAM-16.07	S617: Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) Password expiration enabled	Inspected the password configurations for a sample of in-scope systems during the period to determine that passwords for each in-scope system was configured according to the Company's policy and Company policy required the following (unless there was a system limitations): <ul style="list-style-type: none"> • 25 character minimum • Sufficient randomness (entropy) Password expiration enabled	No exceptions noted.
IAM-16.08	S621: Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
IAM-16.09	S622: Internal user access accounts are created in AD or LDAP authentication systems as part of a defined IAM process.	Inspected the IAM policies and procedures to determine that internal user accounts were created in AD or LDAP authentication systems as part of a defined IAM process.	No exceptions noted.
IAM-16.10	S623: Privileged customer administrator accounts are created in the application based on a written authorization request from the designated customer point of contact.	Inspected the written authorization requests for a sample of customer administrator accounts provisioned during the period to determine that privileged customer administrator accounts were created in the application based on a written authorization request from the designated customer point of contact for each customer administrator account sampled.	No exceptions noted.

INTEROPERABILITY AND PORTABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IPY-01: Interoperability and Portability Policy and Procedures - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: <ul style="list-style-type: none"> a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
IPY-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IPY-01.02	I111: The Company uses open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Inspected the API documentation form from the customer-facing website to determine that the Company used open and published APIs to ensure support for interoperability between components and to facilities migrating applications.	No exceptions noted.
IPY-01.03	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IPY-02: Application Interface Availability - Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.			
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
IPY-02.01	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
IPY-02.02	I111: The Company uses open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Inspected the API documentation form from the customer-facing website to determine that the Company used open and published APIs to ensure support for interoperability between components and to facilities migrating applications.	No exceptions noted.
IPY-02.03	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.
CCM: IPY-03: Secure Interoperability and Portability Management - Implement cryptographically secure and standardized network protocols for the management, import and export of data.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
IPY-03.01	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
IPY-03.02	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IPY-03.03	I111: The Company uses open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Inspected the API documentation form from the customer-facing website to determine that the Company used open and published APIs to ensure support for interoperability between components and to facilities migrating applications.	No exceptions noted.
IPY-03.04	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.
CCM: IPY-04: Data Portability Contractual Obligations - Agreements must include provisions specifying CSCs access to data upon contract termination and will include: <ul style="list-style-type: none"> a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy 			
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
IPY-04.01	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
IPY-04.02	S651: Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IPY-04.03	C115: The company establishes written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the company established written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
IPY-04.04	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
IPY-04.05	I111: The Company uses open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Inspected the API documentation form from the customer-facing website to determine that the Company used open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	No exceptions noted.
IPY-04.06	I112: Policies, procedures, and mutually agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	Inspected the customer facing website to determine that policies, procedures, and mutually agreed upon provisions and/or terms were established to satisfy customer (tenant) requirements for application development, data retrieval, and modification of settings and configuration.	No exceptions noted.

INFRASTRUCTURE AND VIRTUALIZATION SECURITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IVS-01: <i>Infrastructure and Virtualization Security Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
IVS-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-01.02	S343: The company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process and configuration to determine that the company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
IVS-01.03	S664: The Company has documented system hardening standards.	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.
IVS-01.04	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in Technical Operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in Technical Operations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IVS-02: <i>Capacity and Resource Planning</i> - Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.			
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
IVS-02.01	A111: Application errors and processing capacity are monitored continuously, and the monitoring tool generates alerts when specific, predefined thresholds are met.	Inspected the monitoring tool configurations and an example alert to determine that application errors and processing capacity were monitored continuously, and the monitoring tool generated alerts when specific, predefined thresholds were met.	No exceptions noted.
IVS-02.02	S725: An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific, predefined thresholds are met.	Inspected the IT infrastructure monitoring tool configurations and an example alert to determine that an IT infrastructure monitoring tool was utilized to monitor IT infrastructure availability and performance and generated alerts when specific, predefined thresholds were met.	No exceptions noted.
CCM: IVS-03: <i>Network Security</i> - Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
IVS-03.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
IVS-03.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-03.03	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually, and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IVS-03.04	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.
IVS-03.05	S669: WAF software is utilized to identify and alert administrators of any potential web application attacks (see OWASP Top 10) by applying a set of rules to HTTP(S) connections to monitor the underlying web servers.	Inspected the WAF configurations to determine that WAF software is utilized to identify and alert administrators of any potential web application attacks by applying a set of rules to HTTPS connections to monitor underlying web servers.	No exceptions noted.
IVS-03.06	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
IVS-03.07	S726: Media containing confidential information is required to be protected against unauthorized access, misuse, or corruption during transportation.	Inspected the data classification policy to determine that media containing confidential information was required to be protected against unauthorized access, misuse, or corruption during transportation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IVS-04: OS Hardening and Base Controls - Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
IVS-04.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-04.02	S343: The company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process and configuration to determine that the company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
IVS-04.03	S664: The Company has documented system hardening standards.	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.
IVS-04.04	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in Technical Operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in Technical Operations.	No exceptions noted.
CCM: IVS-05: Production and Non-Production Environments - Separate production and non-production environments.			
No mapping to SOC 2 TSCs.			
IVS-05.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IVS-05.02	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
CCM: IVS-06: <i>Segmentation and Segregation</i> - Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.			
No mapping to SOC 2 TSCs.			
IVS-06.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-06.02	S343: The company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process and configuration to determine that the company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
IVS-06.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IVS-06.04	S664: The Company has documented system hardening standards.	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.
IVS-06.05	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in Technical Operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in Technical Operations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: IVS-07: <i>Migration to Cloud Environments</i> - Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
IVS-07.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-07.02	S343: The company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process and configuration to determine that the company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
IVS-07.03	S612: Separate environments are used for development, testing, and production. Access to these environments is governed by the Company's access management policies.	Inspected the network configurations and system access listings for the development, testing, and production environments to determine that separate environments were used for development, testing, and production and access to these environments was governed by the Company's access management policies.	No exceptions noted.
IVS-07.04	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
IVS-07.05	S664: The Company has documented system hardening standards.	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.
IVS-07.06	S665: The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IVS-07.07	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in Technical Operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in Technical Operations.	No exceptions noted.
CCM: IVS-08: <i>Network Architecture Documentation</i> - Identify and document high-risk environments.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
IVS-08.01	S215: The Company has documented network diagrams that are available to authorized users upon request.	Inquired of management to determine that the company had documented network diagrams that were available to authorized users upon request.	No exceptions noted.
		Inspected the network diagrams and the internal document repository to determine that the Company had documented network diagrams that were available to authorized users upon request.	No exceptions noted.
IVS-08.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-08.03	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IVS-08.04	S616: Remote access by employees is permitted only through MFA over an encrypted VPN connection.	Inspected the VPN authentication configurations to determine that remote access by employees was permitted only through MFA over an encrypted VPN connection.	No exceptions noted.
IVS-08.05	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.
IVS-08.06	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
CCM: IVS-09: Network Defense - Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.			
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
IVS-09.01	S215: The Company has documented network diagrams that are available to authorized users upon request.	Inquired of management to determine that the company had documented network diagrams that were available to authorized users upon request.	No exceptions noted.
		Inspected the network diagrams and the internal document repository to determine that the Company had documented network diagrams that were available to authorized users upon request.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IVS-09.02	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
IVS-09.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
IVS-09.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
IVS-09.05	S616: Remote access by employees is permitted only through MFA over an encrypted VPN connection.	Inspected the VPN authentication configurations to determine that remote access by employees was permitted only through MFA over an encrypted VPN connection.	No exceptions noted.
IVS-09.06	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
IVS-09.07	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.

LOGGING AND MONITORING

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-01: <i>Logging and Monitoring Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
LOG-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
LOG-01.02	S664: The Company has documented system hardening standards.	Inspected the system hardening procedures to determine that the Company had documented system hardening procedures.	No exceptions noted.
LOG-01.03	S818: Changes to production server hardening standards are required to be reviewed and approved by a senior manager in Technical Operations.	Inspected the production server hardening standards to determine that changes to production server hardening standards were required to be reviewed and approved by a senior manager in Technical Operations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-02: <i>Audit Logs Protection</i> - Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.			
<i>No mapping to SOC 2 TSCs.</i>			
LOG-02.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-02.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-02.03	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-02.04	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.
LOG-02.05	I133: The system monitors and logs customer e-mail data when it is received, processed, and delivered.	Inspected the customer e-mail logging and monitoring configurations to determine that the system monitored and logged customer e-mail data when it was received, processed, and delivered.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-03: <i>Security Monitoring and Alerting</i> - Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
LOG-03.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-03.02	S231: Customers have the option to report operational failures, incidents, problems, concerns, and complaints. The process for customer reporting is described on the customer-facing website and in online system documentation.	Inspected the company website to determine that customers have the option to report operational failures, incidents, problems, concerns, and complaints and the process for customer reporting was described on the customer-facing website and in online system documentation.	No exceptions noted.
LOG-03.03	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-03.04	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-03.05	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
LOG-03.06	S732: All significant security incidents are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
LOG-03.07	I133: The system monitors and logs customer e-mail data when it is received, processed, and delivered.	Inspected the customer e-mail logging and monitoring configurations to determine that the system monitored and logged customer e-mail data when it was received, processed, and delivered.	No exceptions noted.
CCM: LOG-04: <i>Audit Logs Access and Accountability</i> - Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.			
<i>No mapping to SOC 2 TSCs.</i>			
LOG-04.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-04.02	S231: Customers have the option to report operational failures, incidents, problems, concerns, and complaints. The process for customer reporting is described on the customer-facing website and in online system documentation.	Inspected the company website to determine that customers have the option to report operational failures, incidents, problems, concerns, and complaints and the process for customer reporting was described on the customer-facing website and in online system documentation.	No exceptions noted.
LOG-04.03	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
LOG-04.04	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-04.05	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.
LOG-04.06	I133: The system monitors and logs customer e-mail data when it is received, processed, and delivered.	Inspected the customer e-mail logging and monitoring configurations to determine that the system monitored and logged customer e-mail data when it was received, processed, and delivered.	No exceptions noted.
CCM: LOG-05: <i>Audit Logs Monitoring and Response</i> - Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
LOG-05.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-05.02	S231: Customers have the option to report operational failures, incidents, problems, concerns, and complaints. The process for customer reporting is described on the customer-facing website and in online system documentation.	Inspected the company website to determine that customers have the option to report operational failures, incidents, problems, concerns, and complaints and the process for customer reporting was described on the customer-facing website and in online system documentation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
LOG-05.03	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-05.04	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-05.05	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.
LOG-05.06	I133: The system monitors and logs customer e-mail data when it is received, processed, and delivered.	Inspected the customer e-mail logging and monitoring configurations to determine that the system monitored and logged customer e-mail data when it was received, processed, and delivered.	No exceptions noted.
CCM: LOG-06: <i>Clock Synchronization</i> - Use a reliable time source across all relevant information processing systems.			
<i>No mapping to SOC 2 TSCs.</i>			
LOG-06.01	S727: The Company components are configured to use NTP servers, and the clocks are synchronized with an external time source.	Inspected the NTP configuration to determine that the Company components were configured to use NTP servers, and the clocks were synchronized with an external time source.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-07: <i>Logging Scope</i> - Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
LOG-07.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-07.02	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
CCM: LOG-08: <i>Log Records</i> - Generate audit records containing relevant security information.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
LOG-08.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-08.02	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-09: <i>Log Protection</i> - The information system protects audit records from unauthorized access, modification, and deletion.			
<i>No mapping to SOC 2 TSCs.</i>			
LOG-09.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-09.02	S231: Customers have the option to report operational failures, incidents, problems, concerns, and complaints. The process for customer reporting is described on the customer-facing website and in online system documentation.	Inspected the company website to determine that customers have the option to report operational failures, incidents, problems, concerns, and complaints and the process for customer reporting was described on the customer-facing website and in online system documentation.	No exceptions noted.
LOG-09.03	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-09.04	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-09.05	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.
LOG-09.06	I133: The system monitors and logs customer e-mail data when it is received, processed, and delivered.	Inspected the customer e-mail logging and monitoring configurations to determine that the system monitored and logged customer e-mail data when it was received, processed, and delivered.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-10: Encryption Monitoring and Reporting - Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
LOG-10.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-10.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
LOG-10.03	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-10.04	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-11: Transaction/Activity Logging - Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
LOG-11.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-11.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
LOG-11.03	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-11.04	S6114: A policy on the use of cryptographic controls for protection of information is developed and implemented.	Inspected the cryptographic control policy to determine that a policy on the use of cryptographic controls for protection of information was developed and implemented.	No exceptions noted.
CCM: LOG-12: Access Control Logs - Monitor and log physical access using an auditable access control system.			
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
	Cyxtera, Telstra, NaviSite, Equinix, Macquarie, Internet Solutions, Sure International, e-shelter, Cologix, Databank, and NTT are responsible for ensuring that physical access control systems are in place at the data centers to protect production and backup systems, respectively, from physical threats.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: LOG-13: Failures and Anomalies Reporting - Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.			
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
LOG-13.01	S212: A SIEM tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the SIEM tool configurations and an example alert during the period to determine that a SIEM was utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-13.02	S614: A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.
LOG-13.04	S663: SIEM software continually collects firewall logs, parses the entries using defined business rules, and alerts Information Security personnel when a rule is matched. These logs are restricted and prohibited to modify.	Inspected the SIEM system configurations and an example alert to determine that the SIEM software continually collected firewall logs, parsed the entries using defined business rules, and alerted information Security personnel when a rule was matched, and these logs were restricted and prohibited to modify.	No exceptions noted.
LOG-13.04	S732: All significant security incidents are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.

SECURITY INCIDENT MANAGEMENT, E-DISCOVERY, & CLOUD FORENSICS

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: SEF-01: <i>Security Incident Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
SEF-01.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
SEF-01.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
SEF-01.03	S723: Service Delivery (SD) personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: SEF-02: <i>Service Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
SEF-02.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
SEF-02.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
SEF-02.03	S723: Service Delivery (SD) personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: SEF-03: Incident Response Plans - Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
SEF-03.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
SEF-03.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
SEF-03.03	S723: Service Delivery (SD) personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.
CCM: SEF-04: Incident Response Testing - Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
SEF-04.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
SEF-04.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
SEF-04.03	S723: Service Delivery (SD) personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.
SEF-04.04	S741: The incident response plan is tested at least annually.	Inspected the incident response plan test to determine that the incident response plan was tested during the period.	No exceptions noted.
CCM: SEF-05: <i>Incident Response Metrics</i> - Establish and monitor information security incident metrics.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
SEF-05.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
SEF-05.02	S723: SD personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
SEF-05.03	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
SEF-05.04	S742: Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Inspected the security incident documentation for a sample of incidents during the period to determine that proper forensic procedures, including chain of custody, were required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident, and upon notification, customers and/or other external business partners impacted by a security breach shall be given an opportunity to participate as is legally permissible in the forensic investigation for each incident sampled.	No exceptions noted.
SEF-05.05	S743: The Company makes security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Inspected the Company website to determine that the Company made security incident information available to all affected customers and providers periodically through electronic methods.	No exceptions noted.
CCM: SEF-06: Event Triage Processes - Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
SEF-06.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
SEF-06.02	S723: SD personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.
SEF-06.03	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
SEF-06.04	S742: Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Inspected the security incident documentation for a sample of incidents during the period to determine that proper forensic procedures, including chain of custody, were required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident, and upon notification, customers and/or other external business partners impacted by a security breach shall be given an opportunity to participate as is legally permissible in the forensic investigation for each incident sampled.	No exceptions noted.
SEF-06.05	S743: The Company makes security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Inspected the Company website to determine that the Company made security incident information available to all affected customers and providers periodically through electronic methods.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: SEF-07: Security Breach Notification - Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
SEF-07.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
SEF-07.02	S723: SD personnel have defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which may include requests to reset user passwords or notify Company personnel of potential breaches and incidents.	Inspected the internal Service Delivery protocols to determine that SD personnel had defined protocols for recording, resolving, and escalating received telephone and e-mail requests, which included requests to reset user passwords or notify Company personnel of potential breaches and incidents.	No exceptions noted.
SEF-07.03	S732: All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
SEF-07.04	S742: Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Inspected the security incident documentation for a sample of incidents during the period to determine that proper forensic procedures, including chain of custody, were required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident, and upon notification, customers and/or other external business partners impacted by a security breach shall be given an opportunity to participate as is legally permissible in the forensic investigation for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
SEF-07.05	S743: The Company makes security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Inspected the Company website to determine that the Company made security incident information available to all affected customers and providers periodically through electronic methods.	No exceptions noted.
CCM: SEF-08: <i>Points of Contact Maintenance</i> - Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.			
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.			
SEF-08.01	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
SEF-08.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

SUPPLY CHAIN MANAGEMENT, TRANSPARENCY, AND ACCOUNTABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: STA-01: <i>SSRM Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.			
<i>No mapping to SOC 2 TSCs.</i>			
STA-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-01.02	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
CCM: STA-02: SSRM Supply Chain - Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.			
No mapping to SOC 2 TSCs.			
STA-02.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-02.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-02.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-02.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-03: SSRM Guidance - Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.			
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
STA-03.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-03.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-03.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-03.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-04: SSRM Control Ownership - Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.			
No mapping to SOC 2 TSCs.			
STA-04.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-04.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-04.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-04.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: STA-05: SSRM Documentation Review - Review and validate SSRM documentation for all cloud services offerings the organization uses.			
<i>No mapping to SOC 2 TSCs.</i>			
STA-05.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-05.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-05.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-05.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-06: SSRM Control Implementation - Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.			
<i>No mapping to SOC 2 TSCs.</i>			
STA-06.01	S211: Internal audits are performed continuously and are based on specific compliance frameworks and international standards as determined by management. Controls are monitored and reported on the results of information security and privacy measures of performance.	Inquired of management regarding internal audits to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
		Inspected the evidence of the most recent internal audit to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and controls were monitored and reported on the results of information security and privacy measures of performance.	No exceptions noted.
STA-06.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-06.03	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-06.04	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-06.05	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: STA-07: Supply Chain Inventory - Develop and maintain an inventory of all supply chain relationships.			
<i>No mapping to SOC 2 TSCs.</i>			
STA-07.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-07.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-07.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-07.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
STA-07.05	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
CCM: STA-08: <i>Supply Chain Risk Management</i> - CSPs periodically review risk factors associated with all organizations within their supply chain.			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
STA-08.01	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-08.02	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-08.03	S311: The Company has defined and implemented a formal risk management process for evaluating risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	Inspected the risk management process to determine that the company had defined and implemented a formal risk management process for evaluation risks based on identified threats to the security, availability, processing integrity, privacy, and confidentiality of the system.	No exceptions noted.
STA-08.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
STA-08.05	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: STA-09: Primary Service and Contractual Agreement - Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually agreed upon provisions and/or terms: <ul style="list-style-type: none"> • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy 			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
STA-09.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-09.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-09.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-09.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-10: Supply Chain Agreement Review - Review supply chain agreements between CSPs and CSCs at least annually.			
No mapping to SOC 2 TSCs.			
STA-10.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-10.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-10.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-10.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: STA-11: Internal Compliance Testing - Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.			
<i>No mapping to SOC 2 TSCs.</i>			
STA-11.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-11.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-11.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-11.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-12: Supply Chain Service Agreement Compliance - Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.			
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
STA-12.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-12.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-12.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-12.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-13: <i>Supply Chain Governance Review</i> - Periodically review the organization's supply chain partners' IT governance policies and procedures.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
STA-13.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
STA-13.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-13.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-13.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
CCM: STA-14: <i>Supply Chain Data Security Assessment</i> - Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
STA-14.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
STA-14.02	S232: The Company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the service are identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller.	Inspected the customer agreements for a sample of customers during the period to determine that the company's security, availability, processing integrity, privacy, and confidentiality commitments regarding the services were identified in the Legal and Regulatory addendum and considered with all contracts signed between the Company and the customer or reseller for customer sampled.	No exceptions noted.
STA-14.03	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
STA-14.04	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

THREAT AND VULNERABILITY MANAGEMENT

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: TVM-01: <i>Threat and Vulnerability Management Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
TVM-01.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-01.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-01.03	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-01.04	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: TVM-02: <i>Malware Protection Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
TVM-02.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-02.02	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-02.03	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-02.04	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-02.05	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-02.06	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: TVM-03: <i>Vulnerability Remediation Schedule</i> - Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.			
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
TVM-03.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-03.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-03.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-03.04	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
TVM-03.05	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-03.06	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.
TVM-03.07	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-03.08	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: TVM-04: <i>Detection Updates</i> - Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.			
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-04.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-04.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-04.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-04.04	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
TVM-04.05	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-04.06	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-04.07	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-04.08	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: TVM-05: External Library Vulnerabilities - Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.			
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
TVM-05.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-05.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-05.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-05.04	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
TVM-05.05	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-05.06	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.
TVM-05.07	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-05.08	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: TVM-06: <i>Penetration Testing</i> - Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.			
CC4.2 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-06.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-06.02	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
CCM: TVM-07: <i>Vulnerability Identification</i> - Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
TVM-07.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-07.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-07.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-07.04	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-07.05	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-07.06	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.
TVM-07.07	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-07.08	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: TVM-08: <i>Vulnerability Prioritization</i> - Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.			
<i>No mapping to SOC 2 TSCs.</i>			
TVM-08.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-08.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-08.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-08.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
TVM-08.05	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.
TVM-08.06	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-08.07	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-08.08	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-08.09	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: TVM-09: Vulnerability Management Reporting - Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
TVM-09.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-09.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-09.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-09.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
TVM-09.05	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-09.06	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-09.07	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.
TVM-09.08	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-09.09	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: TVM-10: Vulnerability Management Metrics - Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.			
<i>No mapping to SOC 2 TSCs.</i>			
TVM-10.01	S213: Internal vulnerability scans are performed on a quarterly basis. A remediation plan is developed to remediate all vulnerabilities discovered during the vulnerability scans.	Inspected the internal vulnerability scans for a sample of quarters during the period to determine that internal vulnerability scans were performed, and a remediation plan was developed to remediate all vulnerabilities discovered during the vulnerability scans for each quarter sampled.	No exceptions noted.
TVM-10.02	S222: Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
TVM-10.03	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
TVM-10.04	S324: A risk register is documented and updated continuously. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed with documented treatment plans and assigned risk owners.	Inspected the risk register and most recent risk assessment to determine that a risk register was documented and updated continuously and as part of this process, threats and changes to service commitments were identified and the risks were formally assessed with documented treatment plans and assigned risk owners.	No exceptions noted.
TVM-10.05	S342: Penetration testing is performed semi-annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent penetration test to determine that penetration testing was performed semiannually and a remediation plan was developed, and changes were implemented to remediate any potential critical and high vulnerabilities at a minimum.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
TVM-10.06	S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.	No exceptions noted.
TVM-10.07	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.
TVM-10.08	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
TVM-10.09	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.

UNIVERSAL ENDPOINT MANAGEMENT

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: UEM-01: <i>Endpoint Devices Policy and Procedures</i> - Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
UEM-01.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
UEM-01.02	S227: Employees are required to read and accept the Company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.
UEM-01.03	S2212: Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.
CCM: UEM-02: <i>Application and Service Approval</i> - Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.			
<i>No mapping to SOC 2 TSCs.</i>			
UEM-02.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
UEM-02.02	S227: Employees are required to read and accept the Company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.
UEM-02.03	S343: The Company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process to determine that the Company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
UEM-02.04	S685: The ability to install software on workstations and laptops is restricted to authorized local administrators and IT support staff.	Inspected the information security policy and an example software installation ticket to determine that the ability to install software on workstations and laptops was restricted to authorized local administrators and IT support staff.	No exceptions noted.
UEM-02.05	S2212: Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.
CCM: UEM-03: <i>Compatibility</i> - Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.			
<i>No mapping to SOC 2 TSCs.</i>			
UEM-03.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
UEM-03.02	S227: Employees are required to read and accept the Company's information security and acceptable use policies during induction.	Inspected the information security and acceptable use policy acknowledgements for a sample of employees hired during the period to determine that each employee sampled was required to read and accept the company's information security and acceptable use policies during induction.	No exceptions noted.
UEM-03.03	S343: The Company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process to determine that the Company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
UEM-03.04	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.
UEM-03.05	S685: The ability to install software on workstations and laptops is restricted to authorized local administrators and IT support staff.	Inspected the information security policy and an example software installation ticket to determine that the ability to install software on workstations and laptops was restricted to authorized local administrators and IT support staff.	No exceptions noted.
UEM-03.06	S2212: Acceptable Use Policy of the Company outlines employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	Inspected the acceptable use policy to determine that the acceptable use policy of the company outlined employees' responsibilities around the security of Company equipment inside and outside of Company facilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: UEM-04: <i>Endpoint Inventory</i> - Maintain an inventory of all endpoints used to store and access company data.			
<i>No mapping to SOC 2 TSCs.</i>			
UEM-04.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
UEM-04.02	S343: The Company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process to determine that the Company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
UEM-04.03	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
UEM-04.04	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.
UEM-04.05	S685: The ability to install software on workstations and laptops is restricted to authorized local administrators and IT support staff.	Inspected the information security policy and an example software installation ticket to determine that the ability to install software on workstations and laptops was restricted to authorized local administrators and IT support staff.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: UEM-05: <i>Endpoint Management</i> - Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.			
<i>No mapping to SOC 2 TSCs.</i>			
UEM-05.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
UEM-05.02	S343: The Company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process to determine that the Company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.
UEM-05.03	S611: An asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.
UEM-05.04	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.
UEM-05.05	S685: The ability to install software on workstations and laptops is restricted to authorized local administrators and IT support staff.	Inspected the information security policy and an example software installation ticket to determine that the ability to install software on workstations and laptops was restricted to authorized local administrators and IT support staff.	No exceptions noted.
CCM: UEM-06: <i>Automatic Lock Screen</i> - Configure all relevant interactive-use endpoints to require an automatic lock screen.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
No mapping to SOC 2 TSCs.			
UEM-06.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
UEM-06.02	S6113: AD configurations enforce automatic logoff.	Inspected the AD configurations to determine that AD configurations enforced automatic logoff.	No exceptions noted.
CCM: UEM-07: <i>Operating Systems</i> - Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.			
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
UEM-07.01	S214: A configuration management system is in place and monitors for configuration changes, reverts unauthorized changes back to the original state, and alerts administrators when changes occur.	Inspected the configuration tool configuration and example configuration change ticket to determine that a configuration management system was in place and monitored for configuration changes, reverted unauthorized changes back to the original state, and alerted administrators when changes occurred.	No exceptions noted.
UEM-07.02	S343: The Company uses a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing asset and service management commitments and requirements.	Inspected the configuration management process to determine that the Company used a configuration management process to capture key system components, as well as technical and installation specific implementation details, to support ongoing assets and service management commitments and requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
UEM-07.03	<p>S537: The Company software change management process requires that software change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	<p>Inspected the change request tickets for a sample of software changes during the period to determine that the Company software change management process required that each software change request sampled was:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Deployed into the production environment incrementally and monitored at each deployment stage • Assessed for security implications 	No exceptions noted.
UEM-07.04	<p>S538: The Company infrastructure change management process requires that infrastructure change requests are:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	<p>Inspected the change request tickets for a sample of infrastructure changes during the period to determine that the Company infrastructure change management process required that each infrastructure change is:</p> <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production (when applicable) • Reviewed and approved by management (when applicable) 	No exceptions noted.
UEM-07.05	<p>S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.</p>	<p>Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.</p>	No exceptions noted.
UEM-07.06	<p>S667: Linux infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service are hardened against security threats.</p>	<p>Inspected the patching procedures and an example patch ticket to determine that Linux infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that Linux servers supporting the service were hardened against security threats.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
UEM-07.07	S685: The ability to install software on workstations and laptops is restricted to authorized local administrators and IT support staff.	Inspected the information security policy and an example software installation ticket to determine that the ability to install software on workstations and laptops was restricted to authorized local administrators and IT support staff.	No exceptions noted.
UEM-07.08	S6610: Windows infrastructure supporting the service is patched monthly as a result of identified vulnerabilities to help ensure that Windows servers supporting the service are hardened against security threats.	Inspected the patching procedures and an example patch ticket for a sample of months during the period to determine that Windows infrastructure supporting the service was patched for each month sampled as a result of identified vulnerabilities to help ensure that Windows servers supporting the service were hardened against security threats.	No exceptions noted.
CCM: UEM-08: Storage Encryption - Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
UEM-08.01	S226: The Company has documented security policies and procedures that define the information security rules and requirements for the service environment. Security policies and procedures are available for employees on the intranet.	Inspected the information security policy to determine that the Company had documented security policies and procedures that defined the information security rules and requirements for the service environment and security policies and procedures were available for employees on the intranet.	No exceptions noted.
UEM-08.02	S619: Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
UEM-08.03	S671: Internal storage for workstations and laptops is encrypted.	Inspected the employee workstation system configuration to determine that internal storage for workstations and laptops were encrypted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: UEM-09: Anti-Malware Detection and Prevention - Configure managed endpoints with anti-malware detection and prevention technology and services.			
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
UEM-09.01	S683: Antivirus software is installed on workstations, laptops and Microsoft Windows servers supporting such software. All anti-malware systems update on a regular schedule.	Inspected the anti-malware technology configurations to determine that antivirus software was installed on workstations, laptops and Microsoft Windows servers supporting such software and all anti-malware systems updated on a regular schedule.	No exceptions noted.
UEM-09.02	S684: The Company has deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flows into the Linux environment, which actively scans e-mail for malicious software.	Inspected the anti-malware configurations to determine the Company had deployed anti-malware technology with proprietary malware signatures for e-mail traffic that flowed into the Linux environment, which actively scanned e-mail for malicious software.	No exceptions noted.
CCM: UEM-10: Software Firewall - Configure managed endpoints with properly configured software firewalls.			
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
UEM-10.01	S662: External points of connectivity are protected by a firewall and complex network segmentation. There are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	Inspected the firewall configurations and network segmentation configurations to determine that external points of connectivity were protected by a firewall and complex network segmentation and there are several layers of defense to prevent unauthorized external users from gaining access to the Company's internal systems and devices.	No exceptions noted.
UEM-10.02	S666: The Company continuously monitors the Company's network to detect potential security breaches through a combination of secure architecture, web application firewalls (WAFs), and SIEM solutions.	Inspected the system monitoring configuration to determine that the Company continuously monitored the Company's network to detect potential security breaches through a combination of secure architecture, WAFs, and SIEM solutions.	No exceptions noted.
UEM-10.03	S668: Firewall ruleset changes are reviewed and approved by Information Security. Change tickets are created to track any firewall modifications as a result of review.	Inspected the change tickets for a sample of firewall ruleset changes during the period to determine that firewall ruleset changes were reviewed and approved by Information Security and change tickets were created to track any firewall modifications as a result of the review for each firewall ruleset change sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
UEM-10.04	S669: WAF software is utilized to identify and alert administrators of any potential web application attacks (see OWASP Top 10) by applying a set of rules to HTTP(S) connections to monitor the underlying web servers.	Inspected the WAF configurations to determine that WAF software was utilized to identify and alert administrators of any potential web application attacks by applying a set of rules to HTTPS connections to monitor underlying web servers.	No exceptions noted.
CCM: UEM-11: Data Loss Prevention - Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.			
SOC 2 CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
UEM-11.01	C115: The Company establishes written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the Company establishes written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
UEM-11.02	C116: The Company has implemented the Compliance Protect product, which enforces a minimum retention period to help customers meet regulatory compliance requirements such as SEC 17a-4.	Inspected the customer portal to determine that the Compliance Protect product was implemented to enforce a minimum retention period to help ensure customers meet regulatory compliance requirements such as SEC 17a-4.	No exceptions noted.
UEM-11.03	C122: The Company systematically erases confidential information to meet the Company's confidentiality commitments and system requirements.	Inspected the source code used for destruction of confidential information to determine that the Company systematically erased confidential information to meet the Company's confidentiality commitments and system requirements.	No exceptions noted.
UEM-11.04	C125: The Company ensures that, whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.	Inspected the data deletion configurations to determine that the Company ensured that, whenever data storage space was assigned to a cloud service customer, any data previously reside on that storage space was not visible to that cloud customer.	No exceptions noted.
CCM: UEM-12: Remote Locate - Enable remote geo-location capabilities for all managed mobile endpoints.			
No mapping to SOC 2 TSCs.			
UEM-12.01	S611: Asset database is maintained for risk assessment purposes, reviewed at least annually, and referenced directly in all business resilience related activities. Asset owners are identified and define asset categorization for information security purposes as a part of this system.	Inspected the most recent asset database to determine that an asset database was maintained for risk assessment purposes, reviewed during the period, and referenced directly in all business resilience related activities, and asset owners were identified and defined asset categorization for information security purposes as part of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CCM: UEM-13: Remote Wipe - Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.			
<i>No mapping to SOC 2 TSCs.</i>			
UEM-13.01	C122: The Company systematically erases confidential information to meet the Company's confidentiality commitments and system requirements.	Inspected the source code used for destruction of confidential information to determine that the Company systematically erased confidential information to meet the Company's confidentiality commitments and system requirements.	No exceptions noted.
UEM-13.02	C124: Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
UEM-13.03	C125: The Company ensures that, whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.	Inspected the data deletion configurations to determine that the Company ensured that, whenever data storage space was assigned to a cloud service customer, any data previously reside on that storage space was not visible to that cloud customer.	No exceptions noted.
UEM-13.04	C130: Management utilizes remote wipe capabilities on endpoints to ensure the deletion of company data.	Inspected the remote wipe configurations to determine that management utilized remote wipe capabilities on endpoints to ensure the deletion of company data.	No exceptions noted.
CCM: UEM-14: Third-Party Endpoint Security Posture - Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.			
<i>No mapping to SOC 2 TSCs.</i>			
UEM-14.01	S234: Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
UEM-14.02	S325: Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

ADDITIONAL CRITERIA FOR PRIVACY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
P1.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.			
Not Applicable – Providing notice to data subjects regarding privacy practices, including changes in the use of personal information, is the responsibility of the data controller and not Mimecast given its role as a data processor.			
Privacy Criteria Related to Choice and Consent			
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
Not Applicable – Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Privacy Criteria Related to Collection			
P3.1 Personal information is collected consistent with the entity's objectives related to privacy.			
C113	Documents containing restricted information for business processes, systems, and third-party involvement are clearly identified as part of the classification system of the Company.	Inspected the data classification policy and critical assets document to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
C115	The Company established written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the Company established written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
S141	Employees are required to complete security and privacy training during induction. Security and privacy training includes training on the handling of sensitive data and developments in system security concepts and issues.	Inspected the evidence of completed security awareness training for a sample of employees hired during the period to determine that each employee sampled was required to complete security and privacy awareness training during induction and security and privacy training included training on the handling of sensitive data and developments in system security concepts and issues.	No exceptions noted.
P111	Privacy statement is formally documented and made readily available to data subjects, internal personnel and third parties who need them. Privacy statement is documented to include the following practices: <ul style="list-style-type: none"> • Notice • Choice and Consent • Collection • Use, Retention • Access • Disclosure • Security for Privacy • Monitoring and Enforcement 	Inspected the privacy statement to determine that privacy statement was formally documented to data subjects, internal personnel and third parties who needed them and the privacy statement was documented to include the following practices: <ul style="list-style-type: none"> • Notice • Choice and Consent • Collection • Use, Retention • Access • Disclosure • Security for Privacy • Monitoring and Enforcement 	No exceptions noted.
P112	The latest privacy statement is made publicly available on the Company website.	Inspected the privacy statement to determine that the latest privacy statement was made publicly available on the Company website.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P813	Privacy statement is reviewed and approved by management annually.	Inspected the privacy statement to determine that the privacy statement was reviewed and approved by management during the period.	No exceptions noted.
P11a	Mimecast has a Privacy Information Management System which outlines a framework for Personally Identifiable Information to manage data privacy.	Inspected the privacy statement and information security policy to determine that Mimecast had a Privacy Management System which outlined a framework for Personally Identifiable Information to manage data privacy.	No exceptions noted.
<p>P3.2 For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.</p> <p>Not Applicable - Obtaining consent and communicating the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.</p>			
Privacy Criteria Related to Use, Retention, and Disposal			
P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
S613	Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> Network AdCon console Operating system Database Firewall 	Inquired of the management to determine that privileged access to the following in-scope system components was restricted to authorized users with a business need: <ul style="list-style-type: none"> Network AdCon console Operating system Database Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> Network AdCon console Operating system Database Firewall 	No exceptions noted.
S614	A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
S115	Confidentiality and non-disclosure agreements are established with employees that include clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	Inspected the confidentiality and non-disclosure agreements for a sample of employees hired and current employees during the period to determine that confidentiality and non-disclosure agreements were established for each employee sampled that included clearly defined terms, conditions, and responsibilities regarding compliance with applicable laws and minimum-security standards.	No exceptions noted.
S619	Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data store encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
S621	Management performs a semi-annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the most recent access review to determine that management performed a semi-annual access review for the in-scope system components to ensure that access was restricted appropriately, and tickets were created to remove access as necessary in a timely manner.	No exceptions noted.
S665	The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.			
C115	The Company establishes written policies related to the protection and retention of the confidential information it maintains.	Inspected the information asset retention and disposition policy to determine that the Company established written policies related to the protection and retention of the confidential information it maintains.	No exceptions noted.
C117	The Company requires that the customer review and approve the Compliance Protect retention period once the product is enabled and before the retention period is enforced. The Compliance Protect retention period is visible in a read-only state to customers once approved	Inspected the data storage configuration during the period to determine that the Company required that the customer review and approve the compliance protect retention period once the product was enabled and before the retention period was enforced and the compliance protect retention period was visible in a read-only stat to each customer once approved.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C112	Documents containing restricted customer information for business processes, systems, and third-party involvement are clearly identified as part of the classification systems of the Company	Inspected the data classification policy to determine that documents containing restricted information for business processes, systems, and third-party involvement were clearly identified as part of the classification system of the Company.	No exceptions noted.
S618	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
P423	Security documentation is reviewed annually. In the event that improvements are required, previous version are retained for a period of at least six (6) years.	Inspected the security documentation and data storage configurations for a sample of customers to determine that security documentation was reviewed during the period and in the event the improvement were required, previous version were retained for a period of six years.	No exceptions noted.
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P435	The Company has implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	Observed the user process for the identification and deletion of personal information to determine that the Company had implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	No exceptions noted.
C124	Formal data disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected the data disposal procedures to determine that formal data disposal procedures were in place to guide the secure disposal of the Company's and customers' data.	No exceptions noted.
S651	Electronic media containing confidential information is purged or destroyed and certificates of destruction are issued for each device destroyed.	Inspected the certificate of destruction to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued for each device destroyed.	No exceptions noted.
Privacy Criteria Related to Access			
P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
	Not Applicable – Providing access to data subjects is the responsibility of the data controller and not Mimecast given its role as a data processor.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P5.2 The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
	Not Applicable – Correcting, amending, or appending personal information is the responsibility of the data controller and not Mimecast given its role as a data processor.		
Privacy Criteria Related to Disclosure and Notification			
P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
	Not Applicable – Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Mimecast given its role as a data processor.		
P6.2 The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
P621	Authorized and reported unauthorized disclosures of personal information are tracked and logged.	Inspected legal demand response guidance to determine that the Company maintained procedures for tracking and logging unauthorized disclosures.	No exceptions noted.
		Inspected the records of PII disclosures to third parties to determine that authorized and reported unauthorized disclosures of personal information were tracked and logged.	No exceptions noted.
P611	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed, and agreements are in place consistent with the relevant aspects of the Company's privacy policy.	Inspected the Company website and end user registration process to determine that privacy policies or other specific instructions or requirements for handling personal information were communicated to third parties to whom personal information was disclosed, and agreements were in place consistent with the relevant aspects of the Company's privacy policy.	No exceptions noted.
P6.3 The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			
S222	Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
P621	Authorized and reported unauthorized disclosures of personal information are tracked and logged.	Inspected legal demand response guidance to determine that the Company maintained procedures for tracking and logging unauthorized disclosures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the records of PII disclosures to third parties to determine that authorized and reported unauthorized disclosures of personal information were tracked and logged.	No exceptions noted.
P662	Data processing agreements are formally documented and require that the Company notify customers (data controllers) without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) of a declared breach of security.	Inspected the data processing agreement template to determine that data processing agreements were formally documented and required that the Company notify customers (data controllers) without undue delay of a declared breach of security.	No exceptions noted.
P812	Data subject inquiries, complaints, and dispute issues related to PII are tracked in a ticketing system.	Inspected the ticketing system and example ticket to determine that data subject inquiries, complaints, and dispute issues related to PII were tracked in a ticketing system.	No exceptions noted.
S732	All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
P6.4 The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
P611	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed, and agreements are in place consistent with the relevant aspects of the Company's privacy policy.	Inspected the Company website and end user registration process to determine that privacy policies or other specific instructions or requirements for handling personal information were communicated to third parties to whom personal information was disclosed, and agreements were in place consistent with the relevant aspects of the Company's privacy policy.	No exceptions noted.
P652	Third parties supporting the service who misuse personal information are subject to remedial actions.	Inspected the service agreements for a sample of third parties during the period to determine that third parties supporting the service who misuse personal information were subject to remedial actions for each third-party sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
S234	Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
S325	Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P6.5 The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.			
S234	Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
P652	Third parties supporting the service who misuse personal information are subject to remedial actions.	Inspected the service agreements for a sample of third parties during the period to determine that third parties supporting the service who misuse personal information were subject to remedial actions for each third-party sampled.	No exceptions noted.
P621	Authorized and reported unauthorized disclosures of personal information are tracked and logged.	Inspected legal demand response guidance to determine that the Company maintained procedures for tracking and logging unauthorized disclosures.	No exceptions noted.
		Inspected the records of PII disclosures to third parties to determine that authorized and reported unauthorized disclosures of personal information were tracked and logged.	No exceptions noted.
P611	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed, and agreements are in place consistent with the relevant aspects of the Company's privacy policy.	Inspected the Company website and end user registration process to determine that privacy policies or other specific instructions or requirements for handling personal information were communicated to third parties to whom personal information was disclosed, and agreements were in place consistent with the relevant aspects of the Company's privacy policy.	No exceptions noted.
P662	Data processing agreements are formally documented and require that the Company notify customers (data controllers) without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) of a declared breach of security.	Inspected the data processing agreement template to determine that data processing agreements were formally documented and required that the Company notify customers (data controllers) without undue delay of a declared breach of security.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P6.6 The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
S222	Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
S732	All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.
S742	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Inspected the security incident documentation for a sample of incidents during the period to determine that proper forensic procedures, including chain of custody, were required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident, and upon notification, customers and/or other external business partners impacted by a security breach shall be given an opportunity to participate as is legally permissible in the forensic investigation for each incident sampled.	No exceptions noted.
P611	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed, and agreements are in place consistent with the relevant aspects of the Company's privacy policy.	Inspected the Company website and end user registration process to determine that privacy policies or other specific instructions or requirements for handling personal information were communicated to third parties to whom personal information was disclosed, and agreements were in place consistent with the relevant aspects of the Company's privacy policy.	No exceptions noted.
P621	Authorized and reported unauthorized disclosures of personal information are tracked and logged.	Inspected legal demand response guidance to determine that the Company maintained procedures for tracking and logging unauthorized disclosures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the records of PII disclosures to third parties to determine that authorized and reported unauthorized disclosures of personal information were tracked and logged.	No exceptions noted.
P812	Data subject inquiries, complaints, and dispute issues related to PII are tracked in a ticketing system.	Inspected the ticketing system and example ticket to determine that data subject inquiries, complaints, and dispute issues related to PII were tracked in a ticketing system.	No exceptions noted.
P6.7 The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
Not Applicable – Providing an accounting to the data subject of the personal information held and disclosing a data subject's personal information is the responsibility of the data controller and not Mimecast given its role as a data processor.			
Privacy Criteria Related to Quality			
P7.1 The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
S619	Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data storage encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.
S665	The Company has deployed TLS for the transmission of confidential or sensitive information over public networks.	Inspected the TLS configuration to determine that the Company had deployed TLS for the transmission of confidential or sensitive information over public networks.	No exceptions noted.
I121	Customer-related field forms limit input to acceptable values for storage in the database.	Inspected the validation parameters and the validation process to determine that customer-related field forms limited input to acceptable values for storage in the database.	No exceptions noted.
I122	Customer-related field forms prevent submission if mandatory fields have not been completed.	Inspected the validation parameters and the validation process to determine that customer-related field forms limited input to acceptable values for storage in the database.	No exceptions noted.
I133	The system monitors and logs customer e-mail data when it is received, processed, and delivered.	Inspected the customer e-mail logging and monitoring configurations to determine that the system monitored and logged customer e-mail data when it was received, processed, and delivered.	No exceptions noted.
I134	The application administration portal does not give internal personnel the ability to modify customer data.	Inquired of the application administration portal to determine that the application administration portal did not give internal personnel the ability to modify customer data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the application administration portal to determine that the application administration portal did not give internal personnel the ability to modify customer data.	No exceptions noted.
Privacy Criteria Related to Monitoring and Enforcement			
P8.1 The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.			
P814	The Company has a dedicated DPO and Privacy Lawyer responsible for compliance with all applicable privacy laws and regulations.	Inspected the DPO appointment letter to determine that the Company had a dedicated DPO responsible for compliance with all applicable privacy laws and regulations.	No exceptions noted.
P812	Data subject inquiries, complaints, and dispute issues related to PII are tracked in a ticketing system.	Inspected the ticketing system and example ticket to determine that data subject inquiries, complaints, and dispute issues related to PII were tracked in a ticketing system.	No exceptions noted.
P611	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed, and agreements are in place consistent with the relevant aspects of the Company's privacy policy.	Inspected the Company website and end user registration process to determine that privacy policies or other specific instructions or requirements for handling personal information were communicated to third parties to whom personal information was disclosed, and agreements were in place consistent with the relevant aspects of the Company's privacy policy.	No exceptions noted.
S222	Policy and procedural documents for significant processes, which include employee responsibilities for reporting operational failures, incidents, system problems, and concerns (and the process for doing so), are published and made available on the intranet.	Inspected the incident response policy to determine that policy and procedural documents for significant processes, which included employee responsibilities for reporting operational failures, incidents, system problems, and concerns were published and made available on the intranet.	No exceptions noted.
S732	All significant security incidents including potential events that can disrupt business processes are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management until the Company has recovered from the incident.	Inspected the security incidents ticket for a sample of incidents during the period to determine that all significant security incidents including potential events that can disrupt business processes were subject to the incident response plan and were evaluated, logged, tracked, and communicated to affected parties by management until the Company had recovered for each incident sampled.	No exceptions noted.

PRIVACY NOTICE COMMITMENTS

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PNC1.0 Mimecast shall only Process Personal Data on behalf of Customer in accordance with and for the purposes set out in the Instructions, which, for the avoidance of doubt and depending on the Services provided, may include Mimecast (i) providing the Customer with access to and use of the Services; and (ii) if applicable, improving and developing the Services, including but not limited to using Threat Data to train the Service's machine-learning algorithms, the output of which are anonymized and irreversible. Notwithstanding the foregoing, Processing may be required by Union or Member State law to which Mimecast is subject. In such a case, Mimecast shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.			
S613	Privileged access to the following in-scope system components is restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	Inquired of the management to determine that privileged access to the following in-scope system components was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
		Inspected the system component user listings for a sample of in-scope systems during the period to determine that privileged access to each in-scope system sampled was restricted to authorized users with a business need: <ul style="list-style-type: none"> • Network • AdCon console • Operating system • Database • Firewall 	No exceptions noted.
S614	A privileged access monitoring system is utilized to identify user access rights and analyze activity trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the privileged access monitoring tool configuration and an example notification to determine that a privileged access monitoring system was utilized to identify user access rights and analyze activity trends that had a potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
S141	Employees are required to complete security and privacy training during induction. Security and privacy training includes training on the handling of sensitive data and developments in system security concepts and issues.	Inspected the evidence of completed security awareness training for a sample of employees hired during the period to determine that each employee sampled was required to complete security and privacy awareness training during induction and security and privacy training included training on the handling of sensitive data and developments in system security concepts and issues.	No exceptions noted.
PNC2.0 Mimecast shall notify Customer without undue delay (and in no event more than 48 hours, with periodic updates to follow as may be necessary) of a declared breach of security which has led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer's Personal Data which affects the integrity, availability or confidentiality of Customer's Personal Data ("Security Breach"). For the avoidance of doubt, Security Breaches will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems and no notice of the foregoing shall be required. In the event a Security Breach requires notification by Customer to Data Subjects or relevant Regulators, the parties agree to coordinate in good faith on developing the content of any public statements or required notices.			
P621	Authorized and reported unauthorized disclosures of personal information are tracked and logged.	Inspected legal demand response guidance to determine that the Company maintained procedures for tracking and logging unauthorized disclosures.	No exceptions noted.
		Inspected the records of PII disclosures to third parties to determine that authorized and reported unauthorized disclosures of personal information were tracked and logged.	No exceptions noted.
P611	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed, and agreements are in place consistent with the relevant aspects of the Company's privacy policy.	Inspected the Company website and end user registration process to determine that privacy policies or other specific instructions or requirements for handling personal information were communicated to third parties to whom personal information was disclosed, and agreements were in place consistent with the relevant aspects of the Company's privacy policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
S742	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Inspected the security incident documentation for a sample of incidents during the period to determine that proper forensic procedures, including chain of custody, were required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident, and upon notification, customers and/or other external business partners impacted by a security breach shall be given an opportunity to participate as is legally permissible in the forensic investigation for each incident sampled.	No exceptions noted.
P662	Data processing agreements are formally documented and require that the Company notify customers within 48 hours of a security breach.	Inspected the data processing agreement template to determine that data processing agreements were formally documented and required that the Company notify customers (data controllers) without undue delay of a declared breach of security.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PNC3.0 Customer hereby consents to the use of the Third-Party Subcontractors to perform Services. Subcontracting for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the principal obligation related to the processing of Personal Data pursuant to the Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Mimecast agrees that it has written agreements in place with all Third-Party Subcontractors that contains obligations on the Third-Party Subcontractor that are no less onerous on the relevant Third-Party Subcontractor than the obligations on Mimecast under this DPA in respect of the specific Services provided by the Third-Party Subcontractor.			
S234	Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
S325	Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.
S619	Data stores housing sensitive customer data are encrypted at rest with AES 256-bit encryption.	Inspected the data storage encryption configurations to determine that data stores housing sensitive customer data were encrypted at rest with AES 256-bit encryption.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PNC4.0 If Mimecast appoints a new Third-Party Subcontractor or intendsto make any changes concerning the addition or replacement of the Third-Party Subcontractors, it shallprovide Customer with reasonable advance written notice. For the purposes of this Clause 8.2, notice may be provided electronically, including but not limited to posting on the Mimecast administrative console of the Services, a notice on the Trust Center and/or in a e-newsletter sent to Customer (if Customer has subscribed to such e-newsletter via Mimecast's online preference center). If Customer objects to the appointment or replacement of Third-Party Subcontractor in writing based on legitimate data protection grounds within ten (10) days after Mimecast's advanced written notice of a new Third- Party Subcontractor.			
S234	Mimecast has supply chain management policy/procedure and vendor management process where new vendors are reviewed, security checked. Formal agreements are in place with the Company's vendors and related third parties that include appropriate confidentiality commitments for the service provided, where applicable.	Inspected the vendor agreements for a sample of vendors during the period to determine that Mimecast had supply chain management policy/procedure and vendor management process where new vendors were reviewed, security checked and formal agreements were in place with each Company vendor and related third-party that included appropriate confidentiality commitments for the service provided, where applicable for each vendor sampled.	No exceptions noted.
S229	Changes and notifications are communicated to subcontractors via e-mail and any supporting updates are logged within the ticketing systems.	Inspected the listing of changes and notifications for a sample of subcontractors during the period to determine that changes and notifications were communicated for each subcontractor sampled via e-mail and any supporting updates were logged within the ticketing system.	No exceptions noted.
S325	Subservice organizations, including information processing facilities, providing services to the Company are reviewed on a quarterly basis as part of the vendor risk management process. Attestation and certification reports are obtained and evaluated, when available.	Inquired of management to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available.	No exceptions noted.
		Inspected the subservice organization review documentation for a sample of subservice organizations during the period to determine that subservice organizations, including information processing facilities, provided services to the Company were reviewed on a quarterly basis as part of the vendor risk management process and attestation and certification reports were obtained and evaluated, when available for each subservice organization sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PNC5.0 Mimecast shall provide reasonable assistance in response to inquiries from Customer or its Regulator relating to Mimecast's Processing of Customer's Personal Data. Mimecast shall, upon written request from Customer, provide Customer with information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor.			
S211	Internal audits are performed continuously and are based on specific compliance frameworks and international standards as determined by management. Recommendations on how the system can be improved are made to management.	Inquired of management regarding internal audits to determine that internal audits are performed continuously and are based on specific compliance frameworks and international standards as determined by management and recommendations on how the system can be improved are made to management.	No exceptions noted.
		Inspected the continuous monitoring CAP audit report summary to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and recommendations on how the system could be improved were made to management.	No exceptions noted.
		Inspected the continuous monitoring tracker sheet to determine that the Company tracked continuous monitoring items.	No exceptions noted.
		Inspected the continuous monitoring JIRA ticket to determine that the Company reviewed controls when mapping to NIST 800-53.	No exceptions noted.
S313	Control objectives are established using frameworks such as ISO 27001 and SOC 2.	Inspected the continuous monitoring CAP audit report summary to determine that internal audits were performed continuously and were based on specific compliance frameworks and international standards as determined by management and recommendations on how the system could be improved were made to management.	No exceptions noted.
		Inspected the continuous monitoring tracker sheet to determine that the Company tracked continuous monitoring items.	No exceptions noted.
		Inspected the continuous monitoring JIRA ticket to determine that the Company reviewed controls when mapping to NIST 800-53.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
S314	Privacy related inquiries, complaints, and disputes from customers are responded and monitored through resolution.	Inspected the customer inquiries for a sample of customers during the period to determine that privacy related inquiries, complaints, and disputes from customers were responded and monitored through resolution for each customer sampled.	No exceptions noted.
PNC6.0 Upon termination of this DPA in accordance with Clause 11, Mimecast shall, at Customer's request: delete all Personal Data Processed on behalf of Customer, unless applicable laws, regulations, subpoenas or court orders require it to be retained; or assist Customer with the return to Customer of Personal Data and any copies thereof which it is Processing or has Processed upon behalf of Customer. Customer acknowledges and agrees that the nature of the Services mean that Customer may extract a copy of Personal Data at any time during the term of the Agreement.			
P435	The Company has implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	Observed the user process for the identification and deletion of personal information to determine that the Company had implemented a tool for the identification and deletion of personal information to meet the Company's objectives related to privacy.	No exceptions noted.
C125	The Company ensures that, whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer and copies of data are available upon termination.	Inspected the data storage configuration for a sample of customers during the period to determine that the Company ensured that whenever data storage space was assigned to a cloud service customer, any data previously residing on that storage space was not visible to that cloud service customer and copies of data are available upon termination for each customer sampled.	No exceptions noted.