SOC 2®– SOC for Services Organizations: Trust Services Criteria

For

Prophix Software Inc.

On

Prophix Cloud Services

Report on Prophix Software Inc.'s Description of its Prophix Cloud Services System on the Suitability of the Design and Operational Effectiveness of its Controls Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy For the period May 1, 2022 to October 31, 2022

Non-Disclosure Agreement

It is agreed that, in consideration for Prophix' ("the Company" or "the Client") disclosure of this SOC2 Report dated December 15, 2022 (hereinafter referred to as the Proprietary Material), the Customer agrees that the Proprietary Material is, and shall at all times remain, the property of Prophix or, in the case of the independent service auditors' report, KPMG LLP ("KPMG"), and shall be used solely by the Customer and the independent auditors of the Customer in connection with the services performed by Prophix for the Customer. The Customer will not copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of or give the Proprietary Material to any person, firm or corporation. The Customer shall keep the Proprietary Material confidential and shall not disclose the Proprietary Material to another party without first obtaining written permission from a duly authorized officer of Prophix.

The Customer shall restrict use of the Proprietary Material to its employees and independent auditors who are involved in the evaluation of the Proprietary Material.

Prophix®

Contents

1. Independent Service Auditors' Report 4

2. Statement by Management of Prophix 6

3. Prophix's Description of its Cloud Service System 7
- Prophix Software Inc. Overview 7
- Description of Services Provided 7
- Principal Service Commitments and System Requirements 7
- Components of the System Providing Services 8
  - People 9
  - Procedures 9
  - Data 9
  - Software 10
  - Infrastructure 10
- Customer Responsibilities 10
- Complementary User Entity Controls 10
- Complementary Subservice Organization Controls 11
- Relevant Aspects of the Control Environment, Risk Assessment Process, Communication and Information, Monitoring, and Control Activities 12
  - Control Environment 13
  - *Integrity and Ethical Values* 13
  - *Organizational Structure and Assignment of Authority and Responsibility* 13
  - *Governance and Oversight: Executive Management* 14
  - Governance and Oversight: Human Resource Policies and Practices 15
  - Governance and Oversight: New Hire Process 15
  - *Governance and Oversight: Performance Management and Training* 16
  - *Physical Security* 16
  - *Logical Security / Policies and Procedures* 16
  - Communication and Information 22
  - Risk Assessment 23
  - Monitoring Activities 24
  - Control Activities 24
- Identified System Incidents 25
- Changes since the Date of the Last Report 25

4. Trust Services Categories, Criteria, Related Controls, and Tests of Controls 26
- Applicable Trust Services Criteria Relevant to Security 26
- Additional Criteria for Availability 64
- Additional Criteria for Confidentiality 66
- Additional Criteria for Processing Integrity 69
- Additional Criteria for Privacy 73

1. Independent Service Auditors' Report

KPMG LLP
Chartered Professional Accountants
600, de Maisonneuve blvd. West
Suite 1500
Montreal QC H3A 0A3
Tel 514-840-2100
www.kpmg.ca

Independent Service Auditors' Report

To: Management of Prophix Software Inc.

Scope

We have been engaged to report on Prophix Software Inc.'s (Prophix's) accompanying description of its Cloud Service system titled "Prophix's Description of its Cloud Service System" throughout the period of May 1, 2022 to October 31, 2022, 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 of May 1, 2022 to October 31, 2022, to provide reasonable assurance that Prophix'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria*).

Prophix uses a subservice organization to provide cloud-based SaaS solutions. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Prophix, to achieve Prophix's service commitments and system requirements based on the applicable trust services criteria. The description presents Prophix's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Prophix's controls. The description does not disclose the actual controls at the subservice organization. Our engagement did not include the services provided by the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Prophix, to achieve Prophix's service commitments and system requirements based on the applicable trust services criteria. The description presents Prophix's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Prophix's controls. Our engagement did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Prophix 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 Prophix's service commitments and system requirements were achieved. Prophix has provided the accompanying statement titled "Statement by Management of Prophix" (statement) about the description and the suitability of design and operating effectiveness of controls stated therein. Prophix is also responsible for preparing the description and statement, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services 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.

Our Independence and Quality Control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, 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 the evidence we have obtained.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement 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 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 basis for our opinion.

A reasonable assurance engagement to report on 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 or did not operate effectively;

- 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 its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Evaluating the overall presentation of the description; and
- 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 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 ineffective because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects:

a. The description presents Prophix's cloud service system that was designed and implemented throughout the period of May 1, 2022 to October 31, 2022, in accordance with the description criteria;

b. The controls stated in the description were suitably designed throughout the period of May 1, 2022 to October 31, 2022, to provide reasonable assurance that Prophix'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 organization and user entities applied the complementary controls assumed in the design of Prophix's controls throughout that period; and

c. The controls stated in the description operated effectively throughout the period of May 1, 2022 to October 31, 2022, to provide reasonable assurance that Prophix's service commitments and system requirements were achieved based on the applicable trust services

criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Prophix'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 Prophix, user entities of Prophix's cloud service system during some or all of the period of May 1, 2022 to October 31, 2022, practitioners providing services to such user entities 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 user entity controls and 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
- 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 specific users.

*

KPMG LLP

*CPA auditor, public accountancy permit No. A119819
Montreal, Quebec, Canada
December 15, 2022

2. Statement by Management of Prophix

We have prepared the accompanying description of Prophix Software Inc.'s ("Prophix's") Cloud Service system titled "Prophix's Description of its Cloud Service System" throughout the period May 1, 2022 to October 31, 2022 (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 Cloud Service system that may be useful when assessing the risks arising from interactions with Prophix's system, particularly information about system controls that Prophix has designed, implemented, and operated to provide reasonable assurance that its 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*.

Prophix uses a subservice organization to provide cloud-based SaaS solutions. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Prophix to achieve Prophix's service commitments and system requirements based on the applicable trust services criteria. The description presents Prophix's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Prophix's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Prophix, to achieve Prophix's service commitments and system requirements based on the applicable trust services criteria. The description presents Prophix's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Prophix's controls.

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

a. The description presents Prophix's Cloud Service system that was designed and implemented throughout the period May 1, 2022 to October 31, 2022, in accordance with the description criteria;

b. The controls stated in the description were suitably designed throughout the period May 1, 2022 to October 31, 2022, to provide reasonable assurance that Prophix'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 organization and user entities applied the complementary controls assumed in the design of Prophix's controls throughout that period; and

c. The controls stated in the description operated effectively throughout the period May 1, 2022 to October 31, 2022, to provide reasonable assurance that Prophix's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Prophix's controls throughout that period.

Mr. Alok Ajmera
Chief Executive Officer
December 15, 2022
350 Burnhamthorpe Road West, Suite 100
Mississauga, Ontario L5B 3J1

3. Prophix's Description of its Cloud Service System

Prophix Software Inc. Overview

Prophix Software, founded in 1987, began as a software distributor. After years of implementing financial applications, the company's founders, recognized the need for an innovative planning and reporting system; Prophix's Corporate Performance Management software application was born.

The Prophix software application helps financial professionals reframe their everyday challenges into genuine opportunities. Prophix strives to help companies to improve profitability and minimize risk by automating the repetitive tasks and focus on what matters. Budget, plan, forecast, consolidate, and report automatically. To further simplify deployment and offer a superior user experience, the software is delivered to customers through a fully managed software-as-a-service (SaaS) called Prophix Cloud Services that is powered by Amazon Web Services (AWS). The SaaS model offers a strong value proposition to customers by eliminating significant administrative and IT operational overhead, while still delivering enterprise-class functionality and security for corporate performance management.

Description of Services Provided

This description addresses the Cloud Service SaaS offering. Prophix Cloud Services provides the following services, all of which are covered by this report. If a customer of Prophix Cloud Services has not purchased certain services, the portions of the description that cover those services will not be relevant to those customers. For that reason, it is recommended that customers confirm the services they have purchased by contacting their Prophix Cloud Service account executive.

Prophix Cloud Services is comprised of the following:

- Application services for Forecasting, Planning & Analytics (FP&A), Reporting & Analytics, Financial Consolidation (formerly branded as Sigma Conso Consolidation & Reporting), Intercompany Management (formerly branded as Sigma Conso Intercompany), Dashboarding, and Visual Analytics delivered via standard web browser HTML5 interface using a secured, encrypted HTTPS connection;
- Data integration services for managing the import or export of data into or out of the application;
- Managed sandbox environments for use as development/user acceptance testing purposes;
- Infrastructure implementation, management, and monitoring;
- Managed backups and recovery;
- Managed intrusion prevention system (IPS);
- Managed load balancing; and
- Managed firewalling and security.

Principal Service Commitments and System Requirements

Prophix designs its processes and procedures related to Prophix's cloud services to meet its objectives. Those objectives are based on the service commitments that Prophix makes to its user entities, applicable laws and regulations that govern the provision of Prophix's cloud services, and the financial, operational, and compliance requirements that Prophix has established for the Service.

Service commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Service commitments are standardized and include, the following:

- **Security:** Prophix has made commitments to design, implement, and operate controls to support the protection of the System and security of customer data. These commitments are addressed through controls such as data encryption, authentication mechanisms, network security and other relevant security controls;
- **Availability**: Prophix has made commitments related to percentage uptime and connectivity to Prophix platform;
- **Processing Integrity:** Prophix has made commitments to design, implement, and operate controls to support the integrity of information produced by IT information systems such as application input validation, regression testing of key processing, reconciling output values, and investigation of variances exceeding defined thresholds.
- **Confidentiality**: Prophix has made commitments to design, implement, and operate controls to support the confidentiality of customers' data through data classification policy, data encryption and other relevant security controls; and
- **Privacy**: Prophix has made commitments to design, implement, and operate controls to support the protection and collection of information and to comply with good practices.

Prophix establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Prophix's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cloud Service system.

Components of the System Providing Services

Prophix Cloud Services is deployed on Amazon Web Services (AWS) and relies on its global infrastructure (Figure 1) to deliver corporate performance management (CPM) SaaS to customers around the world. Although AWS is a sub-service organization, the controls in place at AWS are not included within the scope of this examination in this report as the 'carve-out' method has been applied while preparing this report.

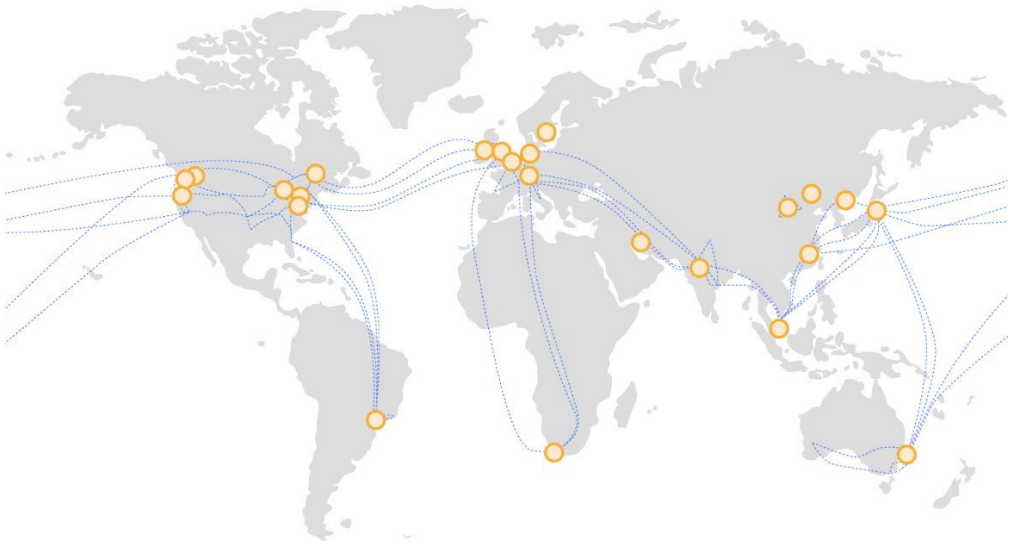


Figure 1-From Amazon Web Services

Data centers, Availability Zones (AZ), and AWS Regions are interconnected via a purpose-built, highly available, and low-latency private global network infrastructure. The network is built on a global, fully redundant, parallel 100 GbE metro fiber network that is linked via trans-oceanic cables across the Atlantic, Pacific, and Indian Oceans, as well as the Mediterranean, Red Sea, and South China Seas.

The choice of exclusively using AWS has been evaluated against a comprehensive set of business and technological decision factors, from robustness of performance, adherence to necessary security and compliance, to availability, and quality of global operational support.

People

Prophix Cloud Services personnel are organized in service teams that develop and maintain Prophix Cloud Services. Members have representation from: Cloud Operations, Information Security, Customer Support, Engineering, Information Technology (IT), Finance, Human Resources (HR), and Executive Management teams. The Operations team consists of the following roles:

- Chief Technology Officer – Executive responsible for reviewing and approving policies and procedures, cloud operations resource management, cross-departmental collaboration, product management, release management, and product strategy;
- Chief Customer Innovation Officer – Executive responsible for the Professional Servicesand Client Services teams, support policies, application-level support escalation management, and customer support resource management;
- Vice-President, Information Security and CISO – Responsibilities include managing security operations, cloud security, audit and compliance, threat analysis, security monitoring, incident management and serves as the Privacy Officer and Change Management review board chair;
- Director, Cloud & Technology Operations – Responsibilities include developing, implementing, and monitoring systems, processes, and technologies for the reliable and scalable operations of Prophix Cloud Services;
- Cloud Operations Engineers – Cloud subject matter experts responsible for leading the development and implementation of cloud automation programs, provisioning and updates, cloud monitoring, configuration management, application support, and on-call/standby support.
- Manager, Customer Support – Responsible for application support, incident management, customer escalations, and support operations resource management;
- Prophix Cloud Services teams are recruited and managed according to Prophix Software policies and procedures.

Procedures

Formal policies and procedures exist that describe incident response, information handling, encryption, and information security standards. Prophix Cloud Services teams are required to adhere to the formal policies and procedures that define how services must be delivered. These are located on the company's intranet and can be accessed by any Prophix Cloud Services team member.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. This data is managed and stored using various database technologies.

Software

Prophix Cloud Services provides cloud services using the regions identified under the heading “Infrastructure,” which supports the application software and underlying operating system software. These are customer dedicated instances that are maintained by Prophix Cloud Services including server backup and recovery, application software updates, patch management, management of the network and platform security firewalls, monitoring, alerting, and load-balancing.

Infrastructure

Prophix Cloud Services are provided to users via cloud service provided by AWS through its global datacenters with failover services provided between data center locations and Availability Zones.

AWS regions are physical locations throughout the world which contain multiple Availability Zones. Availability Zones consist of at least two or more discrete data centers, each with fully redundant power, networking, and connectivity housed in separate secured facilities. These Availability Zones offer the ability to operate production applications, databases, and networks in a highly available, fault tolerant and scalable manner as Availability Zones are connected via fast, private fiber-optic networking - enabling fail-over between Availability Zones without interruption. AWS operates 84 Availability Zones within 26 geographic Regions around the world serving customers in 190 countries.

Customer Responsibilities

Administrator-level user access privileges granted to customers and to their respective environment(s) are initially provided via e-mail using uniquely generated passwords that follow the Prophix Cloud Services standard for secure passwords (at least 8 characters, lower and uppercase letters, one number, and one symbol). The password is paired with the customer’s account information to establish accountability for useractions in the system. In addition, although recommended, at the customer’s discretion, the uniquely generated initial password associated with the customer’s user ID must be changed upon initial login.

Because customers have system administrator-level privileged access to most application-level configurations and can perform logical application security administration functions for their own respective environments, any customer-initiated changes or modifications to the application and logical access entitlements are exclusively the responsibility of these customers.

Prophix Cloud Services customers retain control, stewardship, and ownership of their data.

Prophix Cloud Services requires that a customer’s ability to gain logical access be performed from through encrypted session (HTTPS) and/or from behind a dedicated secure system. It is the customer’s responsibility to maintain all access to their application; this process is excluded from the scope of this report.

Complementary User Entity Controls

Prophix Software applications and systems are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at the user organizations to complement the controls at Prophix. User organizations should consider whether or not the following controls have been placed in operation at the user organizations:

– Controls are in place at user organizations to ensure compliance with contractual requirements;

– Controls are in place to ensure that user organizations accept responsibility for identifying and authenticating all users, for approving access by such users to the services, for controlling against unauthorized access by users, and for maintaining the confidentiality of usernames, passwords andaccount information;

– Controls are in place to accept and provide for the confidentiality and timely and proper termination of user records in user organizations local (intranet) identity infrastructure or on user organizations local computers;

– Controls are in place to notify Prophix immediately of any unauthorized use of Prophix internal or Customer Assets;

– Controls are in place to make every reasonable effort to prevent unauthorized third parties from accessing the Prophix Cloud Services; and

– Controls are in place to ensure that user organizations communicate changes in the designation of individuals who are authorized to instruct Prophix regarding activities on behalf of the user organization.

The list of user organization control considerations presented above do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

Complementary Subservice Organization Controls

Prophix Software Inc. was designed with the assumption that certain control objectives can be achieved only if complementary subservice organization controls assumed in the design of Prophix Software Inc.'s controls are suitably designed and operating effectively, along with the related controls at Prophix Software Inc.

Prophix Software Inc. uses the infrastructure services of AWS to host Prophix Software Inc. and customer data.

For the control objectives listed below, Prophix Software Inc. uses AWS to support the achievement of control objectives identified in this report. The subservice organization controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by the subservice organizations.

Subservice Organization	Criterion	Complementary Subservice Organization Control	AWS Control References
AWS (Amazon Web Services)	CC6.4	Prophix has no physical access to the Amazon Web Services (AWS) physical location. AWS Audit Reports are reviewed by the VP Information Security and CISO. AWS is expected to maintain industry-standard security controls. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS services. Major control areas include: - Data center access limited to authorized data center technicians; - Biometric scanning for controlled data center access; - Security camera monitoring at data center locations; - 24 × 7 onsite staff provide additional protection against unauthorized entry; - Unmarked facilities to help maintain a low profile; - Physical security audited by an independent firm;	AWSCA-4.12 to 4.13 AWSCA-5.1 to 5.5

Subservice Organization	Criterion	Complementary Subservice Organization Control	AWS Control References
		- Cloud infrastructure patch & vulnerability management; - Cloud infrastructure backups and systems monitoring; - Encryption provisions for data at rest and in flight; - Pre-hardened server templates; and - Restricted logical access.	
	A1.2	Environmental protections have been installed including the following: - Cooling systems; - Battery and natural gas generator backup in the event of power failure; - Redundant communications lines; - Smoke detectors; and - Dry pipe sprinklers.	AWSCA-1.10 AWSCA-4.12 AWSCA-5.1 to 5.12
	PI1.3	Operations personnel monitor the status of environmental protections during each shift.	AWSCA-5.3/5.4/5.6/5.8

Relevant Aspects of the Control Environment, Risk Assessment Process, Communication and Information, Monitoring, and Control Activities

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

– **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

– **Communication and Information** – Surrounding these activities are information and communication systems. These enable the entity's people to capture, and exchange information needed to conduct and control its operations.

– **Risk Assessment** – The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.

– **Monitoring Activities** – The entire process must be monitored, and modifications made necessary. In this way, the system can react dynamically, changing as conditions warrant.

– **Control Activities** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's control objectives are effectively carried out.

Set out below is a description of the five components of internal control as it pertains to Prophix.

Control Environment

The objectives of internal control as it relates to Prophix Cloud Services are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant controls, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainderof this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Prophix Cloud Services employees, the policies and procedures, the risk management (RM) process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on Prophix Cloud Services' assessment of risk facing the organization.

Integrity and Ethical Values

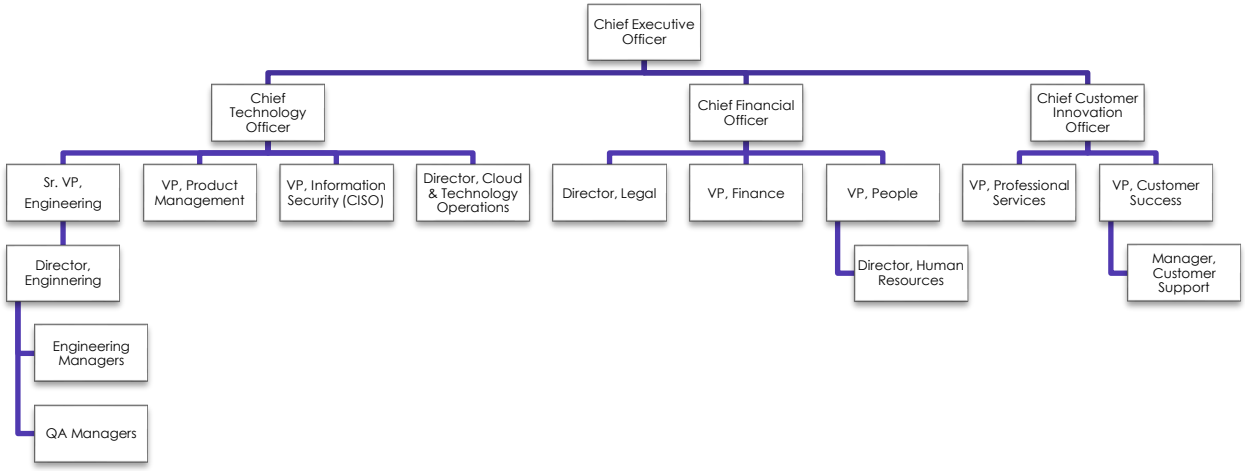
Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior which encompass Prophix Cloud Services, how they are communicated, how they are monitored and enforced in its business activities,are the products of ethical and behavioral standards established by Prophix Software. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

Prophix Software's Executive Management recognize their responsibility to foster a strong ethical environment as it pertains to Prophix Cloud Services to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in Prophix Software's Code of Business Conduct and Ethics (the Code of Conduct), which is distributed to employees of the organization. Specifically, employees and their immediate families are prohibited from using their positions with Prophix for personal or private gain, disclosing confidential information regarding clients, or taking any action that is not in the best interest of clients.

Corporate policy governs employee accounts and transactions are reviewed and monitored to help ensure adherence to Prophix Cloud Services policies. Employees are required to maintain ongoing compliance with statements of policies, procedures, and standards of the Code of Conduct and with lawful and ethical business practices, whether they are specifically mentioned in the Code of Conduct. Employees are required to affirm annually that he or she received, read, understood, and complied with the requirements set forth in the Code of Conduct. Employee recertification status is monitored periodically as part of compliance.

Organizational Structure and Assignment of Authority and Responsibility

The organizational structure of Prophix Software provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Prophix Software has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting. The following organization chart illustrates the defined roles and responsibilities with respect to managing Prophix Cloud Services:



Governance and Oversight: Executive Management

Executive Management, chaired by the Chief Executive Officer ("CEO"), has the responsibility for managing Prophix Cloud Services on a day-to-day basis. Members of Executive Management draw experience from their roles as senior executives of organizations specializing in middle- and back-office support services.

In its role, Executive Management assigns authority and responsibility for operating activities, and establishes reporting relationships and authorization hierarchies. Executive Management designs policies and communications so that personnel understand the objectives of Prophix Cloud Services, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Executive Management convene meetings weekly.

Lines of authority and responsibility are clearly established throughout the organization under Executive Management. These lines of authority and the associated responsibilities are communicated through: (1) management's philosophy and operating style, (2) organizational structure, (3) employee job descriptions, and (4) policy and procedure manuals. Managers are expected to be aware of their responsibilities and lead employees in complying with Prophix Software's policies and procedures. Prophix has a number of policies and procedures designed to help ensure appropriate governance and ethical behaviour, these include:

- Code of Conduct;
- Non-Disclosure Agreements;
- Privacy and Confidentiality Policy;
- Acceptable Use Policy;
- Information Security Management System Policies;
- Recruitment Procedures;
- Risk Management Policy and Procedures;

– Annual Policy Acknowledgement Process; and

– Defined Roles and Responsibilities and have been approved and communicated to personnel.

Governance and Oversight: Human Resource Policies and Practices

Human resources (HR) policies and practices relate to hiring, orienting, training, evaluating, counseling, promoting and compensating personnel. The competence and integrity of Prophix Cloud Services personnel are essential elements of its control environment. The organization's ability to recruit and retain a requisite number of competent and responsible personnel is dependent on its HR policies and processes.

The HR policies and processes of Prophix Software are designed to:

1. Identify and hire competent personnel;
2. Provide employees with the training and information they need to perform their jobs;
3. Evaluate the performance of employees to verify their ability to perform job assignments; and
4. Through performance evaluation, identify opportunities for growth and job performance improvement.

Formal written job descriptions are developed and maintained for positions. Job descriptions are reviewed and updated as needed by relevant management when changes are made to job functions. Changes to formal written job descriptions are submitted to HR for review and approval. Formal written job descriptions are also prepared for contractors who work under the direct supervision of Prophix Cloud Services' management.

Prophix Cloud Services has also established formal classroom instruction, web-based training, and on-the-job employee training programs for critical departments and functions. Programs include orientation on the basics of the functional team's operations, individualized instruction manuals for selected departments, and regularly scheduled department workshops. Employees are also encouraged to actively participate in professional organizations and technical forums to maintain their knowledge and develop awareness of issues facing Prophix Cloud Services.

Governance and Oversight: New Hire Process

Managers within the respective functional groups of the organization determine the need for additional resources and submit formal job requisitions to senior management for approval. Once requisitions have been approved by the appropriate individual(s), HR begins sourcing for the available position. HR screens potential candidates and sends selected résumés to the respective managers. The managers review documentation, select candidates, and inform HR of individuals with whom they wish to schedule interviews and relevant testing if required for the position being filled. The relevant manager and HR conduct interviews and potential offers are submitted to the appropriate authority within the organization for approval.

Individuals offered a position within Prophix Cloud Services are subject to background checks (as appropriate for each country with respect to local regulations) prior to commencing employment. Vendor employees requiring access card/IDs are also subject to background checks. The background check for employees includes substantiation of credentials, previous employment, compensation history and criminal record, as applicable. The background check for vendor employees addresses only criminal record. Prospective employees complete an employment application and sign waivers to release information for the background check. In addition, it is the policy of Prophix Software to request employment references to determine whether the candidate is well-qualified and has the potential to be productive and successful during his or her tenure.

Employees receive data packages containing an overview of Prophix Software's HR policies and procedures. These offer packages include the offer letter or employment contract, the Employee Handbook, relevant compensation materials, benefit materials and the Code of Conduct. Employees are asked in signing their offer to confirm that they have read these materials.

Vendor employees and non-employee personnel must sign an access and use agreement, the terms being similar in nature to the Code of Conduct, prior to being granted access to Prophix Cloud Services.

HR is responsible for managing voluntary and involuntary terminations. Voluntary terminations are identified by the employee's supervisor and are recorded in the event management system. HR personnel communicate with the employee to identify the employee's final day of employment and to inform the employee of his or her rights and responsibilities. The final day is entered in the HR management system and an exit interview is scheduled for that date. During the exit interview, the employee is asked to return any of Prophix Software's company assets in his or her possession, including access card/ID, two-factor authentication token, credit card, laptop, and so on. HR records the information in the event management system and provides the employee with a signed receipt for the items.

Governance and Oversight: Performance Management and Training

Prophix Software has implemented a structured performance appraisal process. Managers are asked to discuss performance expectations and goals with each employee at the start of the year. These objectives and development goals are documented in a performance management system. Prophix Software has a formal mid-year review process and conducts an annual performance review for each employee at the completion of the calendar year. Employees are also required to complete an annual self-appraisal of their performance, attributes, and progress toward stated goals. Annual performance evaluations affirmed by the employee, his or her manager, and director are maintained in electronic form. Managers are also strongly encouraged to have ongoing, informal conversations with employees regarding their performance throughout the year.

Prophix Software has developed mandatory training programs with respect to Security, Confidentiality, and Privacy. These training programs are included as part of the new hire orientation and must be completed annually by personnel. Management monitors compliance to help ensure employees complete the required training. Additional continuing professional education and development opportunities are identified through the goal setting and development-planning process. Managers and HR identify learning plans both by role and level. It is also the manager's role to identify what training an employee requires to comprehend Prophix Software policies and procedures as they relate to specific job requirements. Each employee can partake in formal training classes, on-the-job training, or online education courses. A record of training program attendance is maintained for each employee.

Physical Security

The physical security controls relevant to Prophix cloud service systems are within the AWS data centers environment. AWS is a subservice organization that provides hosting services and the relevant infrastructure resides within its data centers. AWS controls are not in scope of this examination. Further details on the physical security controls can be obtained from the AWS SOC 2 & SOC 3 reports. Following are the control areas that are the responsibility of the subservice organization (AWS):

- Physical Access;
- Fire Detection and Suppression;
- Power;
- Climate and Temperature;
- Device Maintenance and Management; and
- Storage Device Decommissioning.

Logical Security / Policies and Procedures

Organizational Structure

Prophix Cloud Services has implemented an information security management system (ISMS) headed by the Vice-President, Information Security and CISO, under the direction of the Executive Management. The Executive Management team establishes and reviews the security strategy and approves risk management plans, security policies, Information Security organizational structure, and security communication plans. The council also reviews

and approves changes to the system development methodology as it relates to system security and availability and publishes a quarterly security newsletter that is communicated to employees.

Information Security is accountable for the following areas:

– Security architecture;

– Security implementation and change management;

– Security operations and monitoring;

– Security help desk / security incident management; and

– Physical security (where applicable).

Security Policies and Procedures

Prophix Cloud is ISO 27001:2013 Certified and security policies are communicated on the Prophix Cloud Services intranet site, which is available to employees of Prophix Cloud Services. In addition, vendors and vendor personnel with access to the Prophix Cloud Services environment must review and adhere to these policies. Policies are reviewed and updated by the Vice-President, Information Security and CISO, annually and are approved by the Senior Leadership Team. The intranet site includes, but is not limited to, the following policy and procedure elements:

- Information Security Management SystemPolicy
- Information Security Roles Responsibilities andAuthorities
- Procedure for the Control of DocumentedInformation
- Cryptographic Policy
- Physical Security Policy
- Enterprise Security Policy
- General EmergencyPolicy
- Supplier InformationSecurity Evaluation Process
- Network Security Policy
- Secure Development Policy
- Cloud Computing Policy
- Business ContinuityIncident ResponseProcedure
- Wireless CommunicationPolicy
- Server Security Policy
- Procedure for Monitoringthe Use of IT
- Access Control Policy
- Change ManagementProcess
- Availability Management Policy
- IP and Copyright Compliance Policy
- Information SecurityIncident Response
- Process for Monitoring, Measurement, Analysis,and Evaluation
- Procedure for Management Reviews
- Procedure for InternalAudits
- Procedure for theManagement of Nonconformity
- Information Classification Procedure
- Physical Media Transfer Procedure
- Anti-Malware Policy
- Asset HandlingProcedure
- Patch ManagementPolicy
- Technical Vulnerability Management Policy
- Mobile / BYOD DevicePolicy
- Internet Acceptable UsePolicy
- Remote Access / VPN Policy
- Software Policy

Upon hire/initial grant of access, and each January thereafter, employees and vendors are required to complete web-based security awareness, confidentiality, and privacy training programs. Employees have until the end of January to complete training. Completion of security awareness training is tracked via the online delivery vehicle. In addition, as part of this process, employees, and vendors with access to Prophix Cloud Services are required to confirm that they have read the Information Security Polices and accept responsibility for complying with them.

Security Architecture

Prophix Cloud Services utilizes role-based access security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected using native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. Resources are managed in the asset inventory.

Defined configuration standards exist for each hardware platform and each software system and are updated on an as-needed basis (at least annually). Standards are reviewed and approved prior to implementation. Changes are classified as (1) emergency deployment, meaning that they must be deployed on production elements within a defined number of hours /days / weeks, (2) standard deployment, which must be deployed on production elements within a defined number of months, and (3) deploy on rebuild, which is classified as being deployed only when other changes are made to the system configuration. Development servers are updated on a standard deployment or on a rebuild basis.

Secure Network Architecture

Network devices, including firewalls and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface - which manage and enforce the flow of traffic. Prophix Cloud Services approves ACL policies. These policies are automatically pushed, to help ensure these managed interfaces enforce the most up to date.

User Identification and Authentication

Employees and approved vendor personnel sign on to the Prophix Cloud network using a secure user ID and password combination. Users are also required to separately sign on to any systems or applications that do not use any shared sign-on functionality. Passwords must conform to defined password standards and are enforced through parameter settings. These settings are part of the configuration standards and force users to change passwords at a defined interval, disabling the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, requiring an administrator reset of the user ID and password.

Employees and vendors accessing the Prophix Cloud Services network are required to use a two-factor authentication system.

Customers access cloud services through the Internet using the secured, session encrypted functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements.

Access Provisioning / De-provisioning

Upon hire, employees are entered in the HR management system. Access rules are created and are pre- defined based roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for roles are reviewed. In evaluating role access, consideration is given to job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the Vice-President, Information Security and CISO. As part of this process, the Vice-President, Information Security and CISO reviews access by privileged roles and requests for modifications.

Managers may request changes to role access rules. Managers must document the business purpose of the change, risks associated with the change, and consideration of segregation of duties. Senior Management approves access.

Managers may also request a temporary access rule for an individual user for a period up to six months. Approved requests are submitted through the event management system which logs the rules for the specified period.

Access by vendor employees is requested through the temporary access rule system, and access may be granted for periods up to 6 months. Vendor personnel access must be reviewed and approved by the Vice-President, Information Security and CISO prior to processing.

Customer administration accounts are created upon contracting. Customers identify the number of administration accounts needed and the contact information for the primary customer administrator. The contact provides Prophix Cloud security personnel with the names and contact information of the individuals having administration accounts. User IDs are distributed to the contact via telephone, and passwords are communicated directly to the administration account user via telephone.

Accounts are set to “forced” change of password upon initial sign-on.

Administration accounts are unique to each customer environment to give the customer access to their resources while preventing them from accessing other clients’ resources.

Customers are responsible for deletion of customer employee accounts when customer employees are terminated or change responsibilities.

Encryption of Communication Outside the Boundaries

Authorized employees may access the system from the “whitelisted” IP addresses using site-to-site VPN technology. Employees are authenticated using a two-factor authentication system.

Customers interact with their environments through a secure session. Customers are responsible for maintaining access to individuals within their environment.

Prophix Cloud Services uses Amazon Trust Services, a certificate authority, to provide digital certificates used to support encrypted communication.

System Protections

Prophix’s environment is protected against the introduction of malicious or unauthorized software through various control mechanisms.

– Only Prophix Cloud Services administrators can install software. Software is restricted to Prophix approved applications and can only be installed after the appropriate change management approval has been received;

– Cloud Services systems have TrendMicro anti-virus installed. As a policy, every endpoint has antivirus as part of the standard build image and signature files are automatically pushed to the Cloud Service devices;

– Prophix Cloud Services hosts have anti-malware, firewall, Intrusion Prevention Systems (IPS), Host Intrusion Prevention (HIP), Host Intrusion Detection (HID) and File Integrity Monitoring (FIM); and

– The ability to install software on workstations and laptops is restricted to IT support personnel.

Vulnerability Scanning and Assessments

Vulnerability Scanning

Prophix Cloud Services uses both internal personnel and qualified third-party vendors to perform security vulnerability assessment services on its infrastructure and software. A variety of technologies, tools, and techniques are employed to provide broad coverage against various types of threats.

The services are managed by the Vice-President, Information Security and CISO, and CISO, who meets additional stakeholders prior to the start of quarterly testing for planning purposes. As part of this meeting, Prophix Cloud Services provides a current list of infrastructure and software assets. This information is used in planning vulnerability testing. A weekly status meeting is held between the VP Information Security and CISO and stakeholders to monitor the status of the testing and preliminary findings identified.

A closing meeting is held after the completion of testing to formally review the results of testing and remediation plans. This meeting is attended by Executive Management, and the VP of Information Security and CISO. Required personnel and testing tools are granted access only for the period during which testing is performed and are removed upon completion of testing. Logical access is restricted to access needed to perform the functions, and all use of the access is logged.

Vulnerability Scans

Vulnerability scanning is performed - at a minimum – on an annual basis, in accordance with Prophix Cloud Services policy. Prophix utilizes industry standard scanning technologies and a formal methodology to conduct these scans. The technologies are customized to test Prophix Cloud Services' infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis by trained Prophix Cloud Services staff. Scans are performed during non-peak windows. Tools requiring installation in the Prophix Cloud Services system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Testing Results

Reports specifying identified vulnerabilities, a level of assessed risk for the vulnerabilities identified, and suggested remediation are created after vulnerability scans. The report includes an executive summary, which is disseminated to the Executive Management team.

Individual vulnerabilities identified during vulnerability testing are logged and managed through the incident and change management processes.

System Operations and Monitoring

Prophix Cloud Services utilizes a scalable data engine for machine-generated data as part of its Security Incident and Event Management (SIEM) solution. The Prophix Cloud Services SIEM provides the ability to effectively respond to security and operational incidents by analyzing massive amounts of data from large network and IT infrastructures.

The Prophix Clouds Services SIEM collects indexes and harnesses machine data across the infrastructure in real time, aggregating, monitoring and alerting of security and operational events adapting to a dynamic threat landscape, providing for analytics capabilities, contextual incident response and reducing time-to- threat response mitigation.

The Prophix Cloud Services SIEM solution provides for secured audit trails across firewalls, applications, access control, intrusion detection services, intrusion prevention services, malware detection and other components. The SIEM is configured to monitor and alert on the following with respect to system operations and security:

– System state changes;

– Exception alerts from the external perimeter;

– Firewall ruleset changes;

– System performance, security threats, resource utilization, and unusual system activity; and

– System backups.

Based on reported events, Cloud Services Operations personnel follow defined protocols. Security related events also have defined processes in place which includes IS Event Assessment, IS Event Response, Event Tracking, and automatic incident event escalation. In addition, incidents are discussed during weekly operations meetings and high-risk incidents must have a root cause analysis performed and documented by the VP Information Security and CISO.

The VP information Security and CISO, Security actively kept apprised of threats, network performance, system inventory, and configuration changes by receiving and reviewing weekly reports.

Change Management

Prophix has change controls around system components provides reasonable assurance that changes are adequately managed to mitigate the risks of unauthorized alteration and errors. The following control procedures contribute to this objective:

– Prophix has a change process to define the steps to manage standard, normal, emergency, andmajor changes;

– Changes to system components are documented to address management workflow with review,testing and impact analysis of the change and approval before implementation;

- Management of the business unit must confirm understanding of changes before authorizing them;
- System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, and confidentiality commitments and requirements throughout thechange management process;
- Changes are tracked by regular change management review board, change managementverification as well as automated tools;
- The change review board reviews all changes to the Cloud Services production application software except for MACs;
- All changes that might affect security must be approved by the VP of Information Security and CISO;
- Prophix has established separate environments for the Cloud Services Pre-production/Staging andProduction pods;
- Developers do not have access to production. Only the Cloud Services support team can push fromPre-production/Staging to Production which requires a "Promote to Production" approval;
- System state change is monitored, and alerts are sent via email to the Information Security sharedemail box; and
- The Prophix SIEM will identify and report required patches and updates.

Availability Monitoring

The Security Incident and Event Management (SIEM) actively monitors and reports on processing capacity and availability. Data regarding availability related incidents is generated and analysis of any outages, availability events, and capacity notification is prepared. This report is reviewed during regularly scheduled Prophix Cloud Service operations meetings to help ensure the services provided are meeting or exceeding contracted obligations. Based on the review, additional incident or change management tickets may be created to address any identified issues. In addition, Prophix has implemented the following controls to provide reasonable assurance the system operates as expected and can resume operations in the event of an outage, service disruption or disaster:

- Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy;
- Backups are monitored for failure using an automated system and the incident management process is automatically invoked;
- Business continuity and disaster recovery plans have been developed and updated annually;
- The entity uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility; and
- Business continuity and disaster recovery plans, including restoration of backups, are tested annually.

Processing Integrity

Prophix has a series of controls in place to provide reasonable assurance that the integrity of information produced by IT information systems is timely accurate, complete, accessible, and protected. The controls that achieve this objective are as follows:

- Data required to support use of products or services is identified with the customer through Professional Services engagements - this includes sources of data, data elements, date and time ofpopulation of data;
- Application input validation controls are implemented to only accept valid ranges;
- Mechanisms are in place to reconcile and compare output values, variances that exceed definedthresholds are investigated and reviewed on daily basis by the Operations manager;

- Application regression testing validates key processing for the application during the changemanagement;
- Weekly full system and daily incremental backups are performed using an automated system;
- Operations personnel monitor the status of environmental protections during each shift;
- Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends;
- Logical access to stored data is restricted to the application and database administrators; and
- A mirror image of application data files is created nightly and stored on a second secure system foruse in recovery and restoration in the event of a system disruption or outage.

Confidentiality

Prophix has established formal information sharing agreements with related parties and vendors, agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors and return and disposal of confidential information when no longer required. Any changes to the confidentiality practices must be approved by the Vice-President, Information Security and CISO, and formally communicated the users, related parties and vendors. Confidential data protected with encryption and logical access controls are configured to restrict access to only include authorized personnel.

Privacy

Prophix customers can capture PII Information within the application or database. The Data Processing Agreement outlines Prophix's role as Data Processor and the customer's role as Data Controller. The main function of Prophix is as follows:

- Assistance with customer's compliance with Data Subject rights, as requested;
- Maintain documentation/record to support any Data Processing, if any;
- Help ensure staff and other processors are compliant;
- Assistance with deletion or return of any Protected Data as instructed by the customer;
- Breach notification, if any; and
- Manage access rights effectively.

Communication and Information

Internal Communication

Information and communication are an integral component of Prophix Cloud Services' internal control system. It is the process of identifying, capturing, and exchanging information in the form and period necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Prophix Cloud Services, the integrity of information produced by the various information systems is timely, accurate, complete, and protected. Information is reported by various information systems as well as through conversations with clients, vendors, and employees.

Regularly scheduled weekly calls and meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held quarterly to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal, as well as conversations with various internal and external colleagues. The following internal processes, procedures, and training materials are available to Cloud Services personnel via Prophix's intranet:

- IT Security Policies and Procedures;

– Policy and Procedures for significant processes, responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available on the intranet;

– A Change Management Process; and

– Security, Confidentiality, and Privacy Awareness Training.

General updates to entity-wide security policies and procedures are usually communicated to the appropriate Prophix Cloud Services personnel via e-mail messages and intranet services. Prophix utilizes both formal and informal methods for corporate-wide communication. Management is involved with day-to-day operations and can provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within the company.

External Communication

For external communications, the company provides 'Terms and Conditions' to customers.

Terms and Conditions

Terms and conditions are presented to provide a mechanism for communicating the terms of service within the company and between the company and customers. The terms and conditions outline terms and payment for services, use of services, enforcement, intellectual property rights, and warranties. Terms of service documents can be found within customer contracts along with various service level agreements, customer responsibilities and procedures.

Obligations that are outlined within the terms of service and Service Level Agreement (SLA) as they relate to security and availability are as follows:

– System availability targets are outlined within the customer contracts;

– Prophix Cloud Services may schedule network maintenance periods resulting in service interruptions. These maintenance periods are announced in advance to the primary technical contact for customer accounts;

– Customer understands and agrees that occasional temporary interruptions of any services may occur as normal events (e.g. In the provision of Internet services which reside outside the demarcation point of Prophix Cloud Services); and

– Indemnification of company and its affiliated parties.

The terms of service are reviewed at least annually or more frequently when deemed necessary. Any changes are reviewed by Executive Management and sent to the Legal and Administration team for execution of the changes. Customers are notified via e-mail of any changes. The customer is not required to accept or agree to any change.

Risk Assessment

Prophix Cloud Services has established a Risk Management (RM) process that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. RM's approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. RM attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management, including the Management Committee.

The process of identifying, assessing, and managing risks is a critical component of Prophix Cloud Services' internal control system. The purpose of Prophix Cloud Services' risk assessment process is to identify, assess, and manage risks that affect the organization's ability to achieve its objectives. The risk assessment is performed quarterly using the Prophix ISO27001 risk assessment as a basis for risk identification, with additional risks that threaten the

achievement of control objectives added as appropriate. Risk Management considers the following risks as part of the identification process:

– Operational, financial, internal reporting, and compliance objectives;

– Changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives; and

– Environmental, regulatory, and technological changes that may have occurred.

Based on the results of the risk assessment, treatment plans, controls, and other risk mitigation activities are performed. To reduce risk to an acceptable level, Prophix has implemented mitigation measures that reduce the likelihood and impact of risk. These measures include, but are not limited to the following:

– Business continuity and disaster recovery plans that are developed, updated, and tested annually;

– Utilizing a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility;

– Security incident and event monitoring software that is used to identify and alert personnel of potential security threats and vulnerabilities, resource utilization, detect unusual system activity or service requests;

– Incident response policies and procedures;

– Comprehensive insurance coverage to protect against threats that may impact business operations;

– Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria;

– Formal information sharing agreements with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors and return and disposal of confidential information when no longer required; and

– The rules that identify the conditions under which third parties would have access to the data provided to Prophix by its customers.

Monitoring Activities

The management of Prophix Cloud Services also monitors controls to consider whether they are operating as intended, and whether they are modified as appropriate for changes in conditions or risks facing the organization. Ongoing monitoring procedures are built into the normal recurring activities of Prophix Cloud Services and include regular management and supervisory activities. Monthly internal control assessments are performed as well as an annual vulnerability scan on the Cloud Services external perimeter. Issues identified through these monitoring activities are tracked and reported to senior management in a timely manner and appropriate corrective actions are taken.

Control Activities

The source of the criteria used in this report is:

TSP section 100A, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Although the trust services criteria and related controls (control activities) to achieve the applicable trust services criteria are present in section 4, "Trust Services Categories, Criteria, Related Controls and Tests of Controls".

Identified System Incidents

No system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more service commitments and system requirements during the period of time covered by the description have been identified.

Changes since the Date of the Last Report

There have been no significant changes to the system / controls during the period May 1, 2022 to October 31, 2022.

4. Trust Services Categories, Criteria, Related Controls and Tests of Controls

Note to Readers: *Although the applicable trust services criteria and related controls are presented in this section, they are an integral part of Prophix's description of its Cloud Services system throughout the period May 1, 2022 to October 31, 2022.*

Applicable Trust Services Criteria Relevant to Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

I. Information during its collection or creation, use, processing, transmission, and storage; and

II. Systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of Prophix's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC1.0 CONTROL ENVIRONMENT			
Trust Services Criteria: CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.A	Cloud Services staff are required to read and formally acknowledge the code of conduct, NDA, confidentiality and privacy practices, acceptable use policy, and information	For a selection of existing cloud services staff inspected the signed NDA and confidentiality forms and training completion confirmation to determine whether they have acknowledged the code of conduct, NDA, confidentiality	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC1.0 CONTROL ENVIRONMENT			
	system policy upon hire, during the onboarding process and annually thereafter.	and privacy practices, the acceptable use policy and Information system policy. Inspected the list of employees to determine whether there were any new employees during the period.	
CC1.1.B	A formal reference check is performed for Cloud Services staff.	For a selection of new hires, inspected relevant documentation and email communications to determine whether a formal reference check is performed.	No exceptions noted.
CC1.1.C	A formal criminal background check is performed for new admin level Cloud Services staff.	For a selection of new hires, inspected relevant documentation and email communications to determine whether a criminal background check is performed.	No exceptions noted.
Trust Services Criteria: CC1.2 The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control. **Trust Services Criteria: CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**			
CC1.3.A	The Prophix Cloud Services organization structure, roles and responsibilities are formally defined, documented and communicated to Cloud Services staff.	Inspected the organizational structure for the cloud services personnel to determine whether roles and responsibilities were formally defined and documented. For a selection of cloud services personnel, inspected email communications from team members confirming their access to the roles and responsibilities page for cloud operations that is available on the company intranet. Inspected the intranet to determine whether job descriptions are posted.	No exceptions noted.
CC1.3.B	Job descriptions for Prophix Cloud Services are defined by Prophix management to accurately describe the responsibilities of each position.	For a selection of cloud services personnel, inspected job descriptions to determine whether responsibilities of positions are accurately described.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC1.0 CONTROL ENVIRONMENT			
CC1.3.C	Job descriptions are reviewed by management on an as needed basis including when changes are made to any jobs.	For a selection of job description changes, inspected email communication to determine whether they had been reviewed by management.	No exceptions noted.
Trust Services Criteria: CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.1.B	A formal reference check is performed for new Cloud Services staff.	For a selection of new hires, inspected relevant documentation and email communications to determine whether a formal reference check is performed.	No exceptions noted.
CC1.1.C	A formal criminal background check is performed for new admin level Cloud Services staff.	For a selection of new hires, inspected relevant documentation and email communications to determine whether a criminal background check is performed.	No exceptions noted.
CC1.4.A	Cloud Services staff undergo bi-annual competency reviews.	For a selection of cloud services personnel, inspected supporting documentation to determine whether bi-annual competency review was performed during the attestation period.	No exceptions noted.
CC1.4.B	The organization reviews the experience and qualifications of Cloud Operational staff and confirms the candidate's acceptance prior to hiring the individual.	For a selection of new hires, inspected email communications to determine whether the organization reviews the experience and qualifications of Cloud Operational staff and whether a confirmation of the candidate's acceptance prior to hiring is in place.	No exceptions noted.
CC1.4.C	Management establishes requisite skills and promotes continuing education and training for its employees.	For a selection of cloud services personnel, inspected training completion confirmations on the intranet to determine whether they performed the training for security, availability, processing integrity, confidentiality and privacy requirements.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC1.0 CONTROL ENVIRONMENT			
CC1.4.D	Management monitors compliance with Security, Availability, Processing integrity, confidentiality, and Privacy training requirements.	For a selection of cloud services personnel, inspected training completion confirmations on the intranet to determine whether they performed the training for security, availability, processing integrity, confidentiality and privacy requirements. Inquired with the HR Manager and were informed that once the limit date has passed an HR representative will send the completion reports for the teams to the respective managers by email. Inspected the email communications between the HR representative and the Senior Information Security and Compliance Analyst to determine whether it includes information on the training status.	No exceptions noted.
CC1.4.E	Senior management develops a list of characteristics that would preclude employee candidate from being hired based on sensitivity or skill requirements for the given position.	Inspected job descriptions of cloud services positions to determine whether they include description of skill requirements for potential candidates.	No exceptions noted.
Trust Services Criteria: CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.4.A	Cloud Services staff undergo bi-annual competency reviews, additionally all new Application Development hires undergo relevant test scenarios before a job offer is made.	See CC1.4, control CC1.4A.	No exceptions noted.
CC1.5.A	The roles and responsibilities for designing, developing, implementing, operating, maintaining, monitoring, and approving the Prophix Cloud Services controls are defined in written job descriptions, and includes	For a selection of cloud services personnel with an oversight on information security, inspected relevant job descriptions to determine whether roles and responsibilities of positions is accurately described and include aspects of security, availability, processing integrity, privacy and confidentiality.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC1.0 CONTROL ENVIRONMENT			
	aspects of Security, Availability, Processing integrity, Privacy and Confidentiality.		
CC1.5.B	The roles and responsibilities for designing, developing, implementing, operating, maintaining, monitoring, and approving the Prophix Cloud Services controls are communicated to all Cloud Services staff.	For a selection of cloud services personnel, inspected email communications from team members confirming their access to the roles and responsibilities page for cloud operations that is available on the company intranet posted on Confluence. Inspected the intranet to determine whether job descriptions are posted on Confluence.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC2.0 COMMUNICATION AND INFORMATION			
Trust Services Criteria: CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.A	The integrity of information produced by Information Systems is timely, accurate, complete, accessible, and protected.	Inspected logical access restrictions, process flow and operational documentation and procedures, data and application backup configuration settings, system inventory listings, and monitoring software to determine whether the integrity of information produced by information systems is timely, accurate, complete, accessible, and protected.	No exceptions noted.
CC3.1.C	A formal risk assessment of the cloud services environment is conducted quarterly.	See CC3.1, control CC3.1.C.	No exceptions noted.
CC3.2.A	An annual vulnerability scan is performed on the Cloud Services external perimeter. The vulnerabilities identified are reviewed and high-risk items are tracked and resolved.	See CC3.2, control CC3.2.A.	No exceptions noted.
CC4.1.A	Internal control assessments are performed by information security personnel on a monthly basis and the results are reported to senior management.	See CC4.1, control CC4.1.A.	No exceptions noted.
Trust Services Criteria: CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC1.1.A	Cloud Services staff are required to read and formally acknowledge the code of conduct, NDA, confidentiality and privacy practices, acceptable use policy, and information system policy upon hire, during the onboarding process and annually thereafter.	See CC1.1, control CC1.1.A.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC2.0 COMMUNICATION AND INFORMATION			
CC1.3.A	The Prophix Cloud Services organization structure, roles and responsibilities are formally defined, documented and communicated to Cloud Services staff.	See CC1.3, control CC1.3.A.	No exceptions noted.
CC1.3.B	Job descriptions for Prophix Cloud Services are defined by Prophix management to accurately describe the responsibilities of each position.	See CC1.3, control CC1.3.B.	No exceptions noted.
CC1.3.C	Job descriptions are reviewed by management on an as needed basis including when changes are made to any jobs.	See CC1.3, control CC1.3.C.	No exceptions noted.
CC2.2.A	Weekly internal IT meetings are conducted to review and update controls for designing, developing, implementing, operating, maintaining, and monitoring cloud services systems.	For a selection of weeks, inspected relevant IT meeting minutes to determine whether controls for designing, developing, implementing, operating, maintaining and monitoring cloud services systems were reviewed and updated.	No exceptions noted.
CC2.2.B	IT security policies and procedures are available to all cloud services staff via Prophix's intranet site and have been approved by management.	Inspected the intranet to determine whether IT security policies and procedures are made available to employees and contractors.	No exceptions noted.
CC2.2.C	The Security Event & Incident Management (SIEM) system monitors the Cloud Services system for security events. System monitoring reports are automatically distributed daily via email to the Information Security shared email box.	Inspected system settings to determine whether the SIEM is configured to monitor the cloud services system for security events and whether system monitoring reports are automatically distributed daily via email to the information security shared email box.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC2.0 COMMUNICATION AND INFORMATION			
CC2.2.D	Policy and procedure documents for significant processes e.g. outages, incident management, security of data, and availability of systems are available on the intranet.	Inspected the intranet to determine whether IT security policies and procedures including incident management, security of data and systems' availability policies and procedures are posted.	No exceptions noted.
CC2.2.F	All Cloud Services staff are required to attend Security Awareness training during the onboarding process and annually thereafter.	For a selection of new hires and current employees, inspected relevant documentation to determine whether they attended the security awareness training during the onboarding process.	No exceptions noted.
CC2.2.G	Personnel are required to attend annual security, confidentiality, and privacy training.	For a selection of cloud services personnel, inspected training completion confirmations on the intranet to determine whether they performed the training for security, confidentiality and privacy requirements.	No exceptions noted.
CC2.2.I	A change management process document defines the Prophix change management process and method for submitting change requests. Prophix internal support staff and clients are notified about system changes that affect them prior to implementation, via a calendar notification.	Inspected the change management policies and procedures to determine whether the change management process and method for submitting change requests are outlined. Inspected the Prophix release website https://status.prophix.cloud to determine whether a schedule of planned releases is publicly available at least 30 days in advance of expected release dates.	No exceptions noted.
CC2.2.J	Management of the business unit must confirm understanding of changes before authorizing them.	For a selection of changes to the system, inspected relevant change tickets and testing scenarios and results to determine whether management of the business unit confirmed understanding of changes before authorizing them.	No exceptions noted.
CC2.2.K	IT runbooks document information regarding the design and operational details of system controls. Runbooks are available for the cloud services team on Prophix's Intranet.	Inspected the intranet to determine whether IT runbooks are available for the cloud services team.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC2.0 COMMUNICATION AND INFORMATION			
		Inspected a selection of IT runbooks to determine whether they document information regarding the design and operational details of system controls.	
CC2.2.L	A mechanism is in place and posted on the corporate intranet for the enablement of anonymous and confidential communication.	Inspected the intranet to determine whether Prophix employees can submit anonymous feedback.	No exceptions noted.
CC2.2.M	Objectives and responsibilities are clearly communicated via Quarterly Director and Manager Reviews as presented by Senior Management. Additionally, Corporate objectives are communicated to all staff via bi-annual town hall meetings.	For a selection of quarters inspected the Director and Manager review meeting minutes to determine whether objectives and responsibilities had been communicated. Inspected the bi-annual townhall agenda to determine whether corporate objectives had been communicated.	No exceptions noted.
Trust Services Criteria: CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.A	The Prophix external user responsibilities are contained in the client contract.	Inspected the general terms for Prophix cloud services that are publicly available in the Prophix url https://legal.prophix.com/PSI-CST/ and included in customer contracts to determine whether external user responsibilities are contained in the contract.	No exceptions noted.
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	Inspected email communications and SOC 2 reports of related parties and vendors to determine whether their systems were reviewed as part of the vendor risk management process.	No exceptions noted.
CC2.3.C	Customer SLAs / Contracts contain information regarding the design and operation of the system and its boundaries.	Inspected the general terms for Prophix cloud services that are publicly available in Prophix url https://legal.prophix.com/PSI-CST/ and included in customer contracts to determine whether a description of design and operation of the system and its boundaries are outlined.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC2.0 COMMUNICATION AND INFORMATION			
CC2.3.D	The entity's security, availability, processing integrity, confidentiality and privacy commitments regarding the system are included in the master services agreement and customer specific service level agreements. In addition, a summary of these commitments is available on the entity's customer facing website.	Inspected the general terms for Prophix cloud services that are publicly available in Prophix url https://legal.prophix.com/PSI-CST/ to determine whether security, availability, processing integrity, confidentiality and privacy commitments regarding the system are included.	No exceptions noted.
CC2.3.E	The customer process for reporting operational failures, incidents, problems, concerns and complaints, is available on the Prophix support portal (www.prophix.com).	Inspected the intranet to determine whether the process for reporting operational failures, incidents, problems, concerns and complaints is available.	No exceptions noted.
CC2.3.F	Updated system documentation is published on the customer website and intranet 30 days prior to implementation.	Inspected the change management policies and procedures to determine whether change management process and method for submitting change requests are outlined. Inspected the Prophix release website https://status.prophix.cloud to determine whether a schedule of planned releases is publicly available at least 30 days in advance of expected release dates.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC3.0 RISK ASSESSMENT			
Trust Services Criteria: CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. **Trust Services Criteria: CC3.2 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.**			
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	See CC2.3, control CC2.3.B.	No exceptions noted.
CC2.3.D	The entity's security, availability, processing integrity, confidentiality and privacy commitments regarding the system are included in the master services agreement and customer specific service level agreements. In addition, a summary of these commitments is available on the entity's customer facing website.	See CC2.3, control CC2.3.D.	No exceptions noted.
CC3.3.A	The entity has defined and implemented a formal risk management process that specifies business objectives (operational, external financial, external non-financial, internal reporting and compliance objectives) to enable the identification of risks and associated risk tolerances and the process for evaluating risks based on identified	See CC3.3, control CC3.3.A.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC3.0 RISK ASSESSMENT			
	threats and the specified tolerances. Fraud is also considered in assessing risk.		
CC3.1.A	A risk management assessment and treatment process exists and has been adopted for the cloud.	For a selection of quarters, inspected the risk register to determine whether the risk assessment of the cloud services environment was performed and whether treatment processes for identified risks are in place.	No exceptions noted.
CC3.1.B	The risk management assessment and treatment review is an agenda item in the management review meeting.	For a selection of quarters, inspected quarterly meeting minutes to determine whether risk management assessment and treatment review is an agenda item in the management review meeting.	No exceptions noted.
CC3.1.C	A formal risk assessment of the cloud services environment is conducted quarterly.	For a selection of quarters, inspected the risk register to determine whether the risk assessment of the cloud services environment was performed and whether treatment plans for identified risks are in place.	No exceptions noted.
CC3.1.D	The Vice-President, Information Security and CISO, maintains a formal risk policy and risk monitoring process for identifying and assessing the key risks related to security, availability, confidentiality, privacy and processing integrity, and the framework for implementing mitigation strategies.	Inspected the "information security risk assessment and treatment process" policy to determine whether it includes a description of the risk monitoring process for identifying and assessing key risks related to security, availability, confidentiality, privacy and processing integrity, and the framework for implementing mitigation strategies.	No exceptions noted.
CC3.2.A	An annual vulnerability scan is performed on the Cloud Services external perimeter. The vulnerabilities identified are reviewed and high-risk items are tracked and resolved.	Inspected the annual vulnerability scan report to determine whether the scan was performed covering cloud services external perimeters and whether there were high-risk items.	No exceptions noted.
Trust Services Criteria: CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.A	The entity has defined and implemented a formal risk management process that specifies business objectives (operational,	For a selection of quarters, inspected the risk register to determine whether the risk assessment of the cloud services environment was performed and	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC3.0 RISK ASSESSMENT			
	external financial, external non-financial, internal reporting and compliance objectives) to enable the identification of risks and associated risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Fraud is also considered in assessing risk.	whether treatment processes for identified risks, including fraud risks, are in place.	
Trust Services Criteria: CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.A	A risk assessment process has been established. System changes are reviewed and approved by the Change Review Board (CRB).	Inspected the change management process document to determine whether it includes a description of the risk monitoring process for identifying and assessing key risks related to security, availability, confidentiality, privacy and processing integrity, and the framework for implementing mitigation strategies. For a selection of change review board meetings, inspected relevant meeting minutes to determine whether system changes impacting information security, capacity, service continuity plans and release management are assessed and approved by the CRB prior to the deployment of the change.	No exceptions noted.
CC3.4.B	During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	For a selection of quarters, inspected the risk register to determine whether the risk assessment of the cloud services environment was performed and whether it includes changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and whether potential threats to system objectives were updated during the attestation period.	No exceptions noted.
CC3.4.C	During the risk assessment and management process, risk management office personnel identify environmental,	For a selection of quarters, inspected the risk register to determine whether the risk assessment of the cloud services environment was performed and	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC3.0 RISK ASSESSMENT			
	regulatory, and technological changes that have occurred.	whether it includes environmental, regulatory, and technological changes that have occurred during the attestation period.	

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC4.0 MONITORING ACTIVITIES			
Trust Services Criteria: 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.			
CC1.4.A	Cloud Services staff undergo bi-annual competency reviews, additionally all new Application Development hires undergo relevant test scenarios before a job offer is made.	See CC1.4, control CC1.4.A.	No exceptions noted.
CC3.2.A	An annual vulnerability scan is performed on the Cloud Services external perimeter. The vulnerabilities identified are reviewed and high-risk items are tracked and resolved.	See CC3.2, control CC3.2.A.	No exceptions noted.
CC4.1.A	Internal control assessments are performed by information security personnel on a monthly basis and the results are reported to senior management.	For a selection of months, inspected the internal control assessment documents to determine whether the assessment identified risks, likelihood, impact, risk level and a relevant treatment plan that is approved by the SVP of Product and Technology.	No exceptions noted.
Trust Services Criteria: CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.			
CC4.2.A	The entity has a process in place to communicate internal control deficiencies in a timely manner to senior management to take appropriate corrective actions.	For a selection of months, inspected the internal control assessment documents to determine whether the assessment identified risks, likelihood, impact, risk level and a relevant treatment plan that is approved by the SVP of Product and Technology.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC5.0 CONTROL ACTIVITIES			
Trust Services Criteria: CC5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC3.1.C	A formal Risk Assessment of the Cloud Services environment is conducted quarterly.	See CC3.1, control CC3.1.C.	No exceptions noted.
CC3.1.D	The Vice-President, Information Security and CISO, maintains a formal risk policy and risk monitoring process for identifying and assessing the key risks related to security, availability, confidentiality, privacy and processing integrity, and the framework for implementing mitigation strategies.	See CC3.1, control CC3.1.D.	No exceptions noted.
Trust Services Criteria: CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC3.1.C	A formal Risk Assessment of the Cloud Services environment is conducted quarterly.	See CC3.1, control CC3.1.C.	No exceptions noted.
CC3.1.D	The Vice-President, Information Security and CISO, maintains a formal risk policy and risk monitoring process for identifying and assessing the key risks related to security, availability, confidentiality, privacy and processing integrity, and the framework for implementing mitigation strategies.	See CC3.1, control CC3.1.D.	No exceptions noted.
Trust Services Criteria: CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC1.4.A	Cloud Services staff undergo bi-annual competency reviews, additionally all new	See CC1.4, control CC1.4.A.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC5.0 CONTROL ACTIVITIES			
	Application Development hires undergo relevant test scenarios before a job offer is made.		
CC2.2.A	Weekly internal IT meetings are conducted to review and update controls for designing, developing, implementing, operating, maintaining, and monitoring cloud services systems.	See CC2.2, control CC2.2.A.	No exceptions noted.
CC2.2.C	The Security Event & Incident Management (SIEM) system monitors the Cloud Services system for security events. System monitoring reports are automatically distributed daily via email to the Information Security shared email box.	See CC2.2, control CC2.2.C.	No exceptions noted.
CC2.2.D	Policy and procedure documents for significant processes e.g. outages, incident management, security of data, and availability of systems are available on the intranet.	See CC2.2, control CC2.2.D.	No exceptions noted.
CC5.3.A	The Prophix security commitments to external users are outlined in the Cloud Services contract and SLA.	For a selection of customers, inspected the contracts to determine whether service level terms are defined and included.	No exceptions noted.
CC2.3.D	The entity's security, availability, processing integrity, confidentiality and privacy commitments regarding the system are included in the master services agreement and customer specific service level	See CC2.3, control CC2.3.D.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC5.0 CONTROL ACTIVITIES			
	agreements. In addition, a summary of these commitments is available on the entity's customer facing website.		

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Trust Services Criteria: 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.			
C6.1.A	The Prophix Access Control Policy defines password standards for client user access to the Cloud Services application.	Inspected the Prophix Access Control Policy to determine whether it defines password standards for client access to the Cloud Services system. Inspected production system configuration settings to determine whether the passwords configurations are in line with the policy.	No exceptions noted.
C6.1.B	2-factor Authentication (2FA) is implemented for all Prophix Cloud Services support administrators.	Observed the logon process for Cloud Services support administrators to the bastion hosts and cloud system console to determine whether 2-Factor Authentication is required. Inspected the configuration of the 2FA tool to determine whether Cloud Services support administrators were required to use the tool as part of the authentication process to connect to production hosts.	No exceptions noted.
C6.1.C	Cloud Services firewalls have been configured with real-time deviation alerts.	Inspected the firewall alerting configuration to determine whether alerts are sent upon changes to the configuration.	No exceptions noted.
C6.1.D	Prophix has developed a formal user access management process.	Inspected the user access management process document to determine whether it provided procedures for managing user access.	No exceptions noted.
C6.1.E	Cloud Services support users have unique accounts. There are no test accounts, or generic accounts that can change the Prophix Cloud Services systems or data. Databases are accessed using a shared administrative account, access to the credentials for which is restricted using a password manager.	Inspected the Cloud Services account list to determine whether there were test, shared or generic accounts. For generically-named accounts, inquired with the Senior Vice President, Product Planning & Technology to determine whether they were service accounts. Inspected the password manager to determine whether the shared database administration account is restricted to Cloud Services administrators.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1.F	Role-based access for the Prophix Cloud Services support personnel is defined according a defined role-based access control system.	Inspected the cloud service access provisioning system to determine whether Cloud Services support personnel access to the system is role-based. For a selection of Cloud Services support personnel, inspected their job titles and group assignments to determine whether their level of access to production assets was role-based and commensurate with their role.	No exceptions noted.
CC6.1.G	Prophix automatically monitors for changes to role access privileges. Exception alerting is sent to the Information Security shared email box when changes occur.	Inspected the alerting configuration for the cloud platform access management system to determine whether changes to access privileges for roles cause alerts to be sent to the Information Security shared email box.	No exceptions noted.
CC6.1.H	The Prophix Cloud Services secure, hardened host configuration is established with a "Gold Image", and deployments follow a defined process.	Tested in CC7.1.C.	No exceptions noted.
CC6.1.I	Access is logged, and the logs are aggregated and correlated. Automated alerts are generated for specific triggers and sent via email to the Information Security shared email box.	Inspected the configuration of the cloud platform access logging system to determine whether cloud console accesses are logged and forwarded to the SIEM. Inspected the SIEM to determine whether specific access-related triggers are configured to send alerts to the Information Security shared mailbox.	No exceptions noted.
CC6.1.J	Traffic to the Cloud Services Management Pod is encrypted.	Inspected system settings of Prophix's cloud service environment to determine whether the traffic to the Cloud Services Management Pod was encrypted.	No exceptions noted.
CC6.1.K	Access to the Operations Management Pod is accessible only from white-listed IP addresses.	Inspected system settings to determine whether access to the Operations Management Pod is allowed only from white-listed IP addresses.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1.L	The IS administrators access the SIEM using assigned unique accounts with password controls are as per the Prophix IS Policy. Access to the root account on the Linux box hosting the Cloud Services SIEM is restricted to appropriate staff via sudo.	Inspected the SIEM access logs to determine whether the IS Administrator accesses the SIEM using an assigned unique ID and password. Inspected system settings to determine whether access to the root account on the Linux box hosting the Cloud Services SIEM is restricted to appropriate staff via sudo.	No exceptions noted.
CC6.1.M	The Vice-President, Information Security and CISO, approves the use of shared accounts. Mitigating controls are implemented when possible (for example, required use of sudo when accessing the UNIX root account).	See controls CC6.1.E and CC6.1.L.	No exceptions noted.
CC6.1.N	Application-level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list.	Inspected the Prophix application security configuration module to determine whether it restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list.	No exceptions noted.
CC6.6.E	Transmission of digital output beyond the boundary of the system occurs through the use authorized software supporting the Advanced Encryption Standard.	See CC6.6, control CC6.6.E.	No exceptions noted.
Trust Services Criteria: 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.			
CC6.1.I	Accesses are logged, and the logs are aggregated and correlated. Automated alerts are generated for specific triggers and sent via email to the Information Security shared email box.	See CC6.1, control CC6.1.I.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.2.A	Cloud Services support personnel access to the Cloud Hosting Provider Operations Management Pod is controlled by the Cloud Hosting Provider Identity and Access Management (IAM) system. The Chief Technology Officer creates and removes users based on requests from HR.	Inspected the Cloud Hosting Provider Identity and Access Management (IAM) system to determine whether it is used to manage access for Cloud Services support personnel.	No exceptions noted.
CC6.2.B	For Cloud Services support staff exiting this role, Prophix HR initiates the exit process by sending a checklist to the Cloud Services admin manager. The Active Directory procedures are: reset password, disable the account, remove the account from groups, move the account to a no-access group. Follow-on Security Procedures are: review the exit list and alert on access requests for unauthorized access attempts.	Inspected the Access Control Policy to determine whether the process followed to terminate members of Cloud Services support staff. For a selection of terminated employees, inspected termination checklists and access control systems to determine whether cloud services support personnel's user IDs were removed from production access control systems on the date of HR termination notification.	No exceptions noted.
Trust Services Criteria: 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.			
CC6.2.B	For Cloud Services support staff exiting this role, Prophix HR initiates the exit process by sending a checklist to the Cloud Services admin manager. The Active Directory procedures are: reset password, disable the account, remove the account from groups, move the account to a no-access group. Follow-on Security Procedures are: review the exit list and alert on access requests for unauthorized access attempts.	See CC6.2, control CC6.2.B.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1.F	Role-based access for the Prophix Cloud Services support personnel is defined according a defined role-based access control system.	See CC6.1, control CC6.1.F.	No exceptions noted.
CC6.1.B	2-factor Authentication (2FA) is implemented for all Prophix Cloud Services support administrators.	See CC6.1, control CC6.1.B.	No exceptions noted.
CC6.3.A	User access requests flow through the new-hire checklist.	Inspected the Access Control Policy to determine whether user access requests are documented via the new hire checklist.	No exceptions noted.
CC6.3.B	Access Control Policy defines access review procedures.	Inspected the Prophix Access Control Policy to determine whether it defines access review procedures. Inspected access review documentation to determine whether an access review was performed according to the access review procedures.	No exceptions noted.
CC6.3.C	Formal role-based access controls that limit access to system and infrastructure components are created and these are enforced by the access control system. When it is not possible, authorized user IDs with two factor authentications are used.	See CC6.1, controls CC6.1.F and CC6.1.B.	No exceptions noted.
Trust Services Criteria: 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.			
CC6.4.B	An ID card based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	Observed a walkthrough of physical access to the Prophix office to determine whether a card-based physical access control system was in place at both the perimeter and to access sensitive areas within.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	See CC2.3, control CC2.3.B.	No exceptions noted.
Trust Services Criteria: 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.			
CC6.5.A	Procedures are in place to ensure all data stores are physically destroyed or securely wiped prior to being removed from the premises.	Inspected the Records Retention and Protection Policy to determine whether procedures are described for secure disposal and destruction of physical data stores.	No exceptions noted.
Trust Services Criteria: CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.1.N	Application-level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list.	See CC6.1, control CC6.1.N.	No exceptions noted.
CC6.6.A	The Prophix Cloud Services external perimeter is protected by redundant, software-defined firewalls. The external perimeter configuration is monitored and an alert for any ruleset change is generated and sent to the Information Security shared email box.	Inspected architectural documentation to determine whether it included references to perimeter firewalls. Inspected the configuration of the cloud deployment to determine whether redundant perimeter firewalls were deployed. Inspected the alerting configuration to determine whether alerts would be sent upon changes to the firewall ruleset configuration.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
		Inspected a selection of alerts sent to the Information Security shared email box to determine whether they referenced changes to the firewall deployments.	
CC6.6.B	Prophix Cloud Services sessions are controlled via enforced system timeouts and idle session activity settings.	Inspected the session timeout configuration for RDP and SSH to determine whether idle session settings had been configured.	No exceptions noted.
CC6.6.E	Transmission of digital output beyond the boundary of the system is encrypted using the Advanced Encryption Standard.	For a selection of customer web servers, tested the HTTPS configuration to determine whether it supported the Advanced Encryption Standard.	No exceptions noted.
CC6.7.A	A Prophix Policy for the transmission of sensitive information exists.	See CC6.7, control CC6.7.A.	No exceptions noted.
CC6.7.B	A VPN utilizing MFA is required for Prophix employees to connect to the processing center.	See CC6.7, control CC6.7.B.	No exceptions noted.
Trust Services Criteria: C6.7 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.			
CC6.1.N	Application-level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list.	See CC6.1, control CC6.1.N.	No exceptions noted.
CC6.6.E	Transmission of digital output beyond the boundary of the system occurs through the use of authorized software supporting the advanced encryption standard.	See CC6.6, control CC6.6.E.	No exceptions noted.
CC6.7.A	A Prophix Policy for the transmission of sensitive information exists.	Inspected the Cryptographic Policy to determine whether it addresses the transmission of sensitive information.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.7.B	A VPN utilizing MFA is required for Prophix employees to connect to the processing center.	Inspected the configuration of the VPN concentrator to determine whether multi-factor authentication is implemented. Re-performed VPN connection to determine whether the VPN is required in order to connect to the processing center.	No exceptions noted.
Trust Services Criteria: C6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.A	Only Prophix Cloud Services administrators can install software. Software is restricted to Prophix approved applications and can only be installed after the appropriate change management approval has been received.	Inspected the Software Policy document to determine whether software installation in the Cloud Services environments must follow the change management process. See CC8.1, controls CC8.1.B for change management approvals testing and CC8.1.G for testing of restrictions over which personnel can perform changes.	No exceptions noted.
CC6.8.B	Employee workstations have antivirus installed.	Inspected the Prophix anti-virus policy to determine whether it mandates that anti-malware is required on workstations. For a selection of workstations, inspected the anti-virus configuration to determine whether anti-virus was installed and updated.	No exceptions noted.
CC6.8.C	Antivirus Signature files are automatically pushed by TrendMicro for Cloud Services devices.	Inspected the central antivirus management server configuration to determine whether anti-virus signature files are automatically pushed by TrendMicro for Cloud Services devices.	No exceptions noted.
CC6.8.D	Cloud Services hosts have anti-malware, firewall, Intrusion Prevention Systems (IPS), Host Intrusion Prevention (HIP), Host Intrusion Detection (HID) and File Integrity Monitoring (FIM).	For a selection of production hosts, inspected system settings to determine whether anti-malware, firewall, HIP, HID and FIM modules were installed.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.8.E	The ability to install software on workstations and laptops is restricted to IT support personnel.	Inquired with the IT Infrastructure Manager to determine whether the ability to install software on employee workstations is restricted to IT support personnel. Inspected the membership of the Administrators and Domain Admins Active Directory groups to determine whether their membership were IT support personnel. For a selection of Cloud Support employee workstations, obtained the membership of the Local Administrators group to determine whether the employee had local administration privileges.	No exceptions noted.
CC8.1.A	Prophix has a formal change process to define the steps to manage standard, normal, emergency, and major changes.	See CC8.1, control CC8.1.A. Inspected the Change Management Process document to determine whether the steps to manage standard, normal, emergency and major changes are defined.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC7.0 SYSTEM OPERATIONS			
Trust Services Criteria: 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.			
CC3.2.A	An annual vulnerability scan is performed on the Cloud Services external perimeter. The vulnerabilities identified are reviewed and high-risk items are tracked and resolved.	See CC3.2, control CC3.2.A.	No exceptions noted.
CC6.8.D	Cloud Services hosts have anti-malware, firewall, Intrusion Prevention Systems (IPS), Host Intrusion Prevention (HIP), Host Intrusion Detection (HID) and File Integrity Monitoring (FIM).	See CC6.8, control CC6.8.D.	No exceptions noted.
CC7.1.A	System state change is monitored, and alerts are sent via email to the Information Security shared email box.	For a selection of servers, Inspected the configuration to determine whether the SIEM forwarding agent is installed. Inspected the configuration of the SIEM to determine whether it monitors system state change and whether it is configured to send alerts to the Information Security shared email box. For a selection of system alerts inspected to determine whether an automated notification was sent to the Information Security shared email box, and whether the alert was triaged to establish whether it represented a potential security event.	No exceptions noted.
CC7.1.B	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, and confidentiality commitments and requirements throughout the change management process.	For a selection of system changes, inspected relevant change review board meeting minutes and change log to determine whether system changes impacting information security, capacity, service continuity plans and release management are assessed and approved by the CRB prior to the deployment of the change.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC7.0 SYSTEM OPERATIONS			
CC7.1.C	The Prophix Cloud Services secure, hardened host configuration is established with a "Gold Image", and deployments follow a defined process.	Inspected the cloud server template repository to determine whether "Gold Image" templates are maintained. Inspected the scripts used to deploy hosts to determine whether the "Gold Image" is used.	No exceptions noted.
CC7.1.D	Exception alerts from the Cloud Services external perimeter are automatically emailed to the Information Security shared email box in near-real time.	Inspected the alerting configuration to determine whether exception alerts from the Cloud Services external perimeter are automatically emailed to the Information security shared email box.	No exceptions noted.
CC7.1.E	Weekly on-screen reports regarding threat management, network performance, system inventory, and configuration changes are reviewed for identified anomalies by the Vice-President, Information Security and CISO, or designate.	For a selection of weeks, inspected reports covering threat management, network performance, system inventory, and configuration changes, to determine whether they were reviewed by the VP Information Security and CISO or designate.	No exceptions noted.
CC7.1.F	The SIEM automatically sends reports identifying firewall ruleset changes to the Information Security shared email box.	See CC7.1, control CC7.1.A.	No exceptions noted.
CC7.2.A	Audit logging and monitoring software is used to collect data from infrastructure components including endpoint systems to help detect potential security threats and vulnerabilities. This software sends an event message to the operations center and security organization which will review and open a priority incident or problem ticket in	See CC7.1, control CC7.1.A.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC7.0 SYSTEM OPERATIONS			
	the change management system to record the item.		
CC8.1.C	Changes are tracked by regular change management review board, change management verification as well as automated tools.	See CC8.1, control CC8.1.C.	No exceptions noted.
CC8.1.E	All changes that might affect security must be approved by the Vice-President, Information Security and CISO..	See CC8.1, control CC8.1.E.	No exceptions noted.
Trust Services Criteria: 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.			
CC6.8.D	Cloud Services hosts have anti-malware, firewall, Intrusion Prevention Systems (IPS), Host Intrusion Prevention (HIP), Host Intrusion Detection (HID) and File Integrity Monitoring (FIM).	See CC6.8, control CC6.8.D.	No exceptions noted.
CC7.2.A	Audit logging and monitoring software is used to collect data from infrastructure components including endpoint systems to help detect potential security threats and vulnerabilities. This software sends an event message to the operations center and security organization which will review and open a priority incident or problem ticket in the change management system to record the item.	For a selection of infrastructure components, inspected the monitoring and logging tool installed to determine whether it is continuously monitoring and logging security related information. For a selection of alerts, inspected the documentation to determine whether they had been addressed and resolved in a timely manner.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC7.0 SYSTEM OPERATIONS			
Trust Services Criteria: 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.			
CC7.3.A	The following security functions have been defined: - IS Event Assessment; - IS Event Response; and - Event Tracking in a ticketing system.	Obtained and inspected the Information Security Event Assessment Procedure to determine whether it concerned information security event assessment, response, and incident tracking in a ticketing system.	No exceptions noted.
CC7.3.B	Incidents are discussed at the weekly operations meeting.	For a selection of weekly operations meetings, inspected meeting minutes to determine whether incidents were discussed as part of the weekly agenda.	No exceptions noted.
CC9.2.B	Prophix maintains and reviews a log file of all incidents pertaining to privacy and information leakage.	See CC9.2, control CC9.2.B.	No exceptions noted.
Trust Services Criteria: 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.			
A1.2.B	Backups are monitored for failure using an automated system. The incident management process is invoked to investigate failures.	See A1.2, control A1.2.B.	No exceptions noted.
CC7.3.A	The following security functions have been defined: - IS Event Assessment; - IS Event Response; and - Event Tracking in a ticketing system.	See CC7.3, control CC7.3.A.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC7.0 SYSTEM OPERATIONS			
CC7.3.B	Incidents are discussed at the weekly operations meeting.	See CC7.3, control CC7.3.B.	No exceptions noted.
CC9.1.A	Business continuity and disaster recovery plans have been developed and updated annually.	See CC9.1, control CC9.1.B.	No exceptions noted.
Trust Services Criteria: CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC6.1.H	The Prophix Cloud Services secure, hardened host configuration is established with a "Gold Image", and deployments follow a defined process	See CC6.1, control CC6.1.H.	No exceptions noted.
CC7.1.C	The Prophix Cloud Services secure, hardened host configuration is established with a "Gold Image", and deployments follow a defined process.	See CC7.1, control CC7.1.C.	No exceptions noted.
CC7.3.B	Incidents are discussed at the weekly operations meeting.	See CC7.1, control CC7.1.B.	No exceptions noted.
CC8.1.H	The Prophix SIEM will identify and report whether required patches and updates were deployed successfully.	See CC8.1, control CC8.1.H.	No exceptions noted.
CC7.1.E	Weekly on-screen reports regarding threat management, network performance, system inventory, and configuration changes are reviewed for identified anomalies by the Vice-President, Information Security and CISO, or designate.	See CC7.1, control CC7.1.E.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC7.0 SYSTEM OPERATIONS			
CC8.1.I	Cloud Services high risk incidents have a root cause analysis performed and documented by the VP Information Security and CISO. High risk incident root cause analysis is reviewed by management.	See CC8.1, control CC8.1.I.	No exceptions noted.
CC9.1.A	Business continuity and disaster recovery plans have been developed and updated annually.	See CC9.1, control CC9.1.A.	No exceptions noted.
CC9.1.C	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	See CC9.1, control CC9.1.C.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC8.0 CHANGE MANAGEMENT			
Trust Services Criteria: 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.			
CC7.1.B	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, and confidentiality commitments and requirements throughout the change management process.	See CC7.1, CC7.1.B.	No exceptions noted.
CC7.1.C	The Prophix Cloud Services secure, hardened host configuration is established with a "Gold Image", and deployments follow a defined process.	See CC7.1, CC7.1.C.	No exceptions noted.
CC7.1.E	Weekly on-screen reports regarding threat management, network performance, system inventory, and configuration changes are reviewed for identified anomalies by the VP Information Security and CISO or designate.	See CC7.1, CC7.1.E.	No exceptions noted.
CC8.1.A	Prophix has a formal change process to define the steps to manage standard, normal, emergency, and major changes.	Inspected the Change Management Process document to determine whether the steps to manage standard, normal, emergency and major changes are defined.	No exceptions noted.
CC8.1.B	Changes to system components are documented to address management workflow with review, testing and impact analysis of the change and approval before implementation.	For a selection of changes, inspected change tickets and review documentation to determine whether: - Changes were tested; - An impact analysis had been performed; and - Management authorized the change before implementation.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC8.0 CHANGE MANAGEMENT			
CC8.1.E	All changes that might affect security must be approved by the Vice-President, Information Security and CISO.	For a selection of changes to the system affecting security, inspected relevant change tickets to determine whether an approval from Chief Information Security Officer was obtained.	No exceptions noted.
CC8.1.F	Prophix has established separate environments for the Cloud Services pre production / staging and production pods.	Inspected the network diagram, logical topology diagrams, and logical access listings to determine whether Prophix has established separate testing and production environments. Inspected system settings to determine whether pre-production/staging and Production environments are segregated.	No exceptions noted.
CC8.1.G	Developers do not have access to production. Only the Cloud Services support team can push from Preproduction/Staging to Production which requires a "Promote to Production" approval.	Inspected the Group membership listing of privileged users with access to the production environment to determine whether they also have development access and whether only the Cloud Services support team can push from pre-production/Staging to Production after obtaining the "Promote to Production" approval from the VP Information Security and CISO.	No exceptions noted.
CC8.1.H	The Prophix SIEM will identify and report whether required patches and updates were deployed successfully.	Inspected system settings to determine whether the SIEM is configured to identify and report whether patches and updates had been deployed successfully.	No exceptions noted.
CC8.1.I	Cloud Services high risk incidents have a root cause analysis performed and documented by the Vice-President, Information Security and CISO. High risk incident root cause analysis is reviewed by management.	For a selection of weekly operation review meetings, inspected meeting minutes to determine whether incident management is a standard discussion point. The process of performing a root cause analysis is not tested as there were no high -risk information security incidents during the attestation period.	Unable to test the root cause analysis as there have been no high-risk incidents during the period. No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC9.0 RISK MITIGATION			
Trust Services Criteria: CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC7.3.B	Incidents are discussed at the weekly operations meeting.	See CC7.3, control CC7.3.B.	No exceptions noted.
CC9.1.A	Business continuity and disaster recovery plans have been developed and updated annually.	Inspected the business continuity plan and disaster recovery framework to determine whether they were updated during the period and whether they included the following key points: - Plan Objectives; - Activation Criteria and Procedures; - Implementation Procedure including Business Team and IT Team Recovery Checklists; - Roles, Responsibilities and Authorities of IT Recovery and Customer; Recovery Teams; - Communication Requirements and Procedures; - Internal and External Interdependencies and Interactions; - Resource Requirements; - Information Flow and Documentation Processes; and - Restoration of Normal Service.	No exceptions noted.
CC9.1.B	The entity uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	Inspected the Prophix cloud disaster recovery topology to determine whether Prophix uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility. Inspected the use of separate cloud regions and machine backup strategy to determine whether Prophix uses a multi-location strategy to permit resumption of operations in the event of the loss of a cloud provider facility.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC9.0 RISK MITIGATION			
CC9.1.C	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the cloud Disaster recovery test report to determine whether the business continuity and disaster recovery plans, including restoration of backups, are tested during the last year.	No exceptions noted.
CC9.1.D	The entity has comprehensive insurance coverage to protect against threats that may impact business operations.	Inspected the insurance certificate to determine whether it includes coverage for commercial general liability, umbrella form excess liability, and Professional and Cyber Liability.	No exceptions noted.
CC7.2.A	Audit logging and monitoring software is used to collect data from infrastructure components including endpoint systems to be used for monitoring system performance, potential security threats and vulnerabilities, capacity monitoring, resource utilization, and to detect unusual system activity or service requests. This software sends an event message to the operations center and security organization which will review and open a priority incident or problem ticket and change management system to record the item.	See CC7.2, control CC7.2.A.	No exceptions noted.
Trust Services Criteria: CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.A	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors	For a selection of related parties and vendors, inspected relevant agreements including data processing agreements to determine whether information sharing requirements were outlined. Inspected the following policies and procedures to determine whether guidance on confidentiality of data was included: - Information security for supplier relationships; - Supplier information security agreement; and	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC9.0 RISK MITIGATION			
	and return and disposal of confidential information when no longer required.	- Supplier due diligence assessment.	
CC9.2.B	Prophix maintains and reviews a log file of all incidents pertaining to privacy and information leakage.	Inquired with the Vice-President, Information Security and CISO, and were informed that there were no privacy incidents during the attestation period. Inspected the privacy officer's inbox to determine whether privacy incidents were logged.	No exceptions noted.
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	See CC2.3, CC2.3.B.	No exceptions noted.
CC9.2.D	Vendor and business partner terminations are facilitated through Prophix Legal / Vendor Contract Management – all terminated contracts are reviewed on a bi-annual basis.	Inquired with the Associate Contracts Manager and were informed that there were no terminations of any Cloud Services vendor during the attestation period. Inspected the Information Security for Supplier Relationships document to determine whether it includes steps to be taken for vendor and business partner terminations.	Unable to test. There were no terminations during the period.

Additional Criteria for Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to meet the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by the service organization's systems, as well as the products or services provided to its customers. The availability objective does not set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
Trust Services Criteria: 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.			
A1.1.A	Monitoring software is used to collect data from infrastructure components to monitor system performance and resource utilization. This software sends an event message to the operations center which will review and open a priority incident or problem ticket in the change management system to record the item.	Inspected deployment scripting to determine whether the monitoring system agent is automatically deployed to new customer deployments. For a selection of performance events, inspected the alerting system and change management system to determine whether the events were triaged and resolved.	No exceptions noted.
A1.1.B	Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.	Inquired with the VP Information Security and CISO to determine whether infrastructure components are evaluated for criticality classification and assignment of a minimum level of redundancy. Inspected deployment scripting to determine whether database replication and backup are deployed automatically as part of the new customer deployment process.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
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.			
A1.2.B	Backups are monitored for failure using an automated system. The incident management process is invoked to investigate failures.	Inspected the configuration of the SIEM to determine whether it monitors backup failures and whether it is configured to send alerts to the Information Security shared email box. For a selection of backup failure alerts, inspected emails from operations staff to determine whether backup failures were investigated.	No exceptions noted.
CC9.1.A	Business continuity and disaster recovery plans have been developed and updated annually.	See CC9.1, control CC9.1.A.	No exceptions noted.
CC9.1.B	The entity uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	See CC9.1, control CC9.1.B.	No exceptions noted.
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	See CC2.3, control CC2.3.B.	No exceptions noted.
Trust Services Criteria: A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
CC9.1.C	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	See CC9.1, control CC9.1.C.	No exceptions noted.

Additional Criteria for Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to meet the service organization's service commitments and system requirements.

Confidentiality addresses the service organization's ability to protect information designated as confidential, from its collection or creation through its final disposition and removal from the service organization's control, in accordance with the service organization's service commitments and system requirements. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
Trust Services Criteria: C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.A	The Vice-President, Information Security and CISO, and Legal Department is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to users, related parties, and vendors.	Inquired with the the VP Information Security and CISO and were informed that there were no changes to confidentiality practices and commitments during the attestation period. Inspected the "terms-of-use" and "privacy-policy" documents that are published on Prophix website to determine whether they include processes covering document creation, review, approval, communication, maintenance, archival and disposal as well as records lifecycle.	No exceptions noted.
C1.1.B	Related party and vendor agreements are modified to reflect changes in confidentiality practices and commitments.	Inquired with the VP Information Security and CISO and were informed that there were no changes to confidentiality practices and commitments during the attestation period. Inspected the "terms-of-use" and "privacy-policy" documents that are published on Prophix website to determine whether they include processes covering	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
		document creation, review, approval, communication, maintenance, archival and disposal as well as records lifecycle.	
CC6.6.E	Transmission of digital output beyond the boundary of the system occurs through the use of authorized software supporting the advanced encryption standard.	See CC6.6, control CC6.6.E.	No exceptions noted.
CC9.2.A	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors and return and disposal of confidential information when no longer required.	See CC9.2, control CC9.2.A.	No exceptions noted.
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	See CC2.3, control CC2.3.B.	No exceptions noted.
CC6.1.F	Role-based access for the Prophix Cloud Services support personnel is defined according a defined role-based access control system.	See CC6.1, control CC6.1.F.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
CC6.1.N	Application-level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list.	See CC6.1, control CC6.1.N.	No exceptions noted.
Trust Services Criteria: C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
CC9.2.A	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors and return and disposal of confidential information when no longer required.	See CC9.2, control CC9.2.A.	No exceptions noted.
CC1.2.B	Data retention and destruction policies and procedures are in place and are reviewed annually.	See CC1.2, control CC1.2.B.	No exceptions noted.
P4.3.A	Prophix securely deletes customer information upon termination of contract.	See P4, control P4.3.A.	No exceptions noted.

Additional Criteria for Processing Integrity

The trust services criteria relevant to processing integrity address the need for system processing to be complete, valid, accurate, timely, and authorized to meet the service organization's service commitments and system requirements.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
Trust Services Criteria: 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.			
PI1.1.A	Data required to support use of products or services is identified with the customer through Professional Services engagements - this includes sources of data, data elements, date and time of population of data.	Inspected the following documents to determine whether data required to support the use of products or services is identified: - PROPHIX 101 Guide for Customers; - Dimension & Data Setup Guide; and - Dimension & Data Setup Template. For a selection of customers, inspected relevant email correspondences to determine whether confirmation of services and communication of dimension and data guidance documents took place.	No exceptions noted.
Trust Services Criteria: 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.			
PI1.2.A	Application input validation controls are implemented to only accept valid ranges.	Performed edit checks over the following attributes to determine whether only valid ranges are accepted by the system: - Date; - Dimension member; - List; - Text;	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
		- Numeric, and - True / False.	
Trust Services Criteria: PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
A1.2.B	Backups are monitored for failure using an automated system. The incident management process is invoked to investigate failures.	See A1.2, control A1.2.B.	No exceptions noted.
PI1.3.A	Output values are compared against prior cycle values. Variances are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.	Inspected system settings to determine whether application regression testing, system integration testing and system functional testing are performed and whether identified system bugs are logged as incidents and are followed-up until resolution. For a selection of incidents extracted from the incident management system, inspected relevant tickets to determine whether an investigation was conducted, and the issue was resolved. Inspected variance reports to determine whether Management reviews the monthly change in reported system bugs.	No exceptions noted.
PI1.3.B	Application regression testing validates key processing for the application during the change management process.	Inspected system settings to determine whether application regression testing, system integration testing and system functional testing are performed and whether identified system bugs are logged as incidents and are followed-up until resolution.	No exceptions noted.
PI1.3.C	Weekly full system and daily incremental backups are performed using an automated system.	Inspected system settings to determine whether the system is configured to perform weekly full system and daily incremental backups.	No exceptions noted.
PI1.3.G	Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends.	Inspected weekly IT meeting minutes to determine whether daily, weekly and monthly trend reports were reviewed by the operations manager for unusual trends.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
PI1.3.H	Logical access to stored data is restricted to the Cloud Operations and Customer Support team.	Inspected system settings to determine whether logical access to stored data is restricted to the Cloud Operations and Customer Support team.	No exceptions noted.
PI1.3.I	A mirror image of application data files is created nightly and stored on a second secure system for use in recovery and restoration in the event of a system disruption or outage.	Inspected system settings to determine whether a mirror image of application data files is created nightly and stored on a second secure system in a different availability zone for use in recovery and restoration.	No exceptions noted.
CC2.3.B	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.	See CC2.3, control CC2.3.B.	No exceptions noted.
Trust Services Criteria: PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.			
PI1.3.B	Application regression testing validates key processing for the application during the change management process.	See PI1.3, control PI1.3.B.	No exceptions noted.
PI1.3.G	Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends.	See PI1.3, control PI1.3.G.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
Trust Services Criteria: 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.			
PI1.3.I	A mirror image of application data files is created nightly and stored on a second secure system for use in recovery and restoration in the event of a system disruption or outage.	See PI1.3, control PI1.3.I.	No exceptions noted.

Additional Criteria for Privacy

The trust services criteria relevant to privacy address the need for personal information to be collected, used, retained, disclosed, and disposed to meet the service organization's service commitments and system requirements.

Although the confidentiality criteria applies to various types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized as follows:

i. Notice and communication of objectives. The entity provides notice to data subjects about its objectives related to privacy.

ii. Choice and consent. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

iii. Collection. The entity collects personal information to meet its objectives related to privacy.

iv. Use, retention, and disposal. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.

v. Access. The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

vi. Disclosure and notification. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

vii. Qualify. The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.

viii. Monitoring and enforcement. The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy – related inquiries, complaints, and disputes.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P1.0 Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
Trust Services Criteria: 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.			
P1.1.A	Prophix outlines their obligation within service agreements with each customer including communication of updates.	For a selection of customers, inspected the service agreement to determine whether Prophix's obligation on how they communicate updates to privacy requirements is outlined.	No exceptions noted.
P1.1.B	Internal users are required to read the data processing agreement.	Inspected Prophix's privacy policy shared publicly on https://www.prophix.com/privacy-policy to determine whether data processing obligations by Prophix are outlined. For a selection of cloud services personnel, inspected relevant email confirmations to determine whether they have acknowledged the data processing agreement.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P2.0 Privacy Criteria Related to Choice and Consent			
Trust Services Criteria: 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.			
P2.1.A	Prophix outlines their obligation within the data processing agreement on how they will assist the customer with their obligations. Where applicable, Prophix customers are required to obtain appropriate consent. Agreement with customers is in place with clear declarations of how personal information will be used and with whom these are shared.	For a selection of new customers, inspected the Data Processing Agreement and cloud service agreement to determine whether Prophix's obligation on how they will assist the customer with their obligation is outlined and whether customers are responsible for obtaining consent from their data subjects over collected information and upon each use of the information by Prophix employees or third parties.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P3.0 Privacy Criteria Related to Collection			
Trust Services Criteria: P3.1 Personal information is collected consistent with the entity's objectives related to privacy.			
P3.1.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not collect personal information on behalf of its customers. Personal Information in the Cloud Solution is collected and entered by the customer.	Not tested as this is a user entity control.	Not applicable to Prophix.
Trust Services Criteria: 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.			
P3.2.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not collect any personal information on behalf of its customers. All Personal Information in the Cloud Solution is collected and entered by the customer.	Not tested as this is a user entity control.	Not applicable to Prophix.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P4.0 Privacy Criteria Related to Use, Retention, and Disposal.			
Trust Services Criteria: P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.1.A	Access to personal information is provided to employees on a need-to-know basis and for the purpose of running the required transactions.	Inspected the standard customer agreement to determine whether it includes a clause prohibiting sharing personal and sensitive information by the customer.	No exceptions noted.
Trust Services Criteria: P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.			
P4.2.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not collect any personal information on behalf of its customers. All Personal Information in the Cloud Solution is collected and entered by the customer.	Not tested as this is a user entity control.	Not applicable to Prophix.
Trust Services Criteria: P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P4.3.A	Prophix securely deletes customer information upon termination of contract.	For a selection of terminated customers, inspected their instance status in the system to determine whether relevant customer data had been deleted.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P5.0 Privacy Criteria Related to access.			
Trust Services Criteria: 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.			
P5.1.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not manage access for data subjects.	Not tested as this is a user entity control.	Not applicable to Prophix.
Trust Services Criteria: 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.			
P5.2.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not correct, amend, or append personal information.	Not tested as this is a user entity control.	Not applicable to Prophix.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P6.0 Privacy Criteria Related to disclosure and notification.			
Trust Services Criteria: 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.			
P6.1.A	Prophix's customers are made aware of third parties who have access to their data subjects' personal information.	Inspected Prophix's website to determine whether it includes public information with respect to hosting customer's data on AWS.	No exceptions noted.
Trust Services Criteria: 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.			
P6.2.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not collect any personal information on behalf of its customers. All personal information in the could solution is collected and entered by the customer.	Not tested as this is a user entity control.	Not applicable to Prophix.
Trust Services Criteria: 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.			
CC9.2.B	Prophix maintains and reviews a log file of all incidents pertaining to privacy and information leakage.	See CC9.1, control CC9.2.B.	No exceptions noted.
Trust Services Criteria: 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.			
CC9.2.B	Prophix maintains and reviews a log file of incidents pertaining to privacy and information leakage.	See CC9.2, control CC9.2.B.	No exceptions noted.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P6.0 Privacy Criteria Related to disclosure and notification.			
P6.4.A	Any vendor or third party is subject to the same data processing agreements terms that Prophix has with its customers.	For a selection of vendors or third parties, inspected relevant agreements and privacy requirements to determine whether the vendors or third parties are subject to the same data processing agreement terms that Prophix has with its customers including notifying Prophix of actual or suspected unauthorized disclosures of personal information.	No exceptions noted.
P6.4.B	For vendors and third parties, Prophix assesses the compliance with privacy requirements annually.	Inspected email communications and SOC 2 reports of related parties and vendors to determine whether their systems were reviewed as part of the vendor risk management process.	No exceptions noted.
Trust Services Criteria: 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.			
CC9.2.B	Prophix maintains and reviews a log file of all incidents pertaining to privacy and information leakage.	See CC9.1, control CC9.2.B.	No exceptions noted.
P6.4.A	Any vendor or third party is subject to the same data processing agreements terms that Prophix has with its customers.	For a selection of vendors or third parties, inspected relevant agreements and privacy requirements to determine whether the vendors or third parties are subject to the same data processing agreement terms that Prophix has with its customers including notifying Prophix of actual or suspected unauthorized disclosures of personal information.	No exceptions noted.
Trust Services Criteria: 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.			
P6.6.A	Prophix has a policy of notifying users of breaches and all such communications are retained.	Inspected privacy policies and procedures to determine whether the requirements of notifying users of breaches and the retention of such breaches are outlined.	No exceptions noted.
Trust Services Criteria: 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.			

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P6.0 Privacy Criteria Related to disclosure and notification.			
P6.7.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not interact with data subjects.	Not tested as this is a user entity control.	Not applicable to Prophix.

Control	Description of Prophix's Controls	KPMG's Test of Controls	Results of KPMG's Test of Controls
P7.0 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.			
P7.1.A	This Trust Services principle is not applicable to Prophix's service as outlined in section 3. Prophix does not collect any personal information on behalf of its customers. All personal information in the could solution is collected and entered by the customer.	Not tested as this is a user entity control.	Not applicable to Prophix.

Control	Description of Prophix's Control	KPMG's Test of Controls	Results of KPMG's Test of Controls
P8.0 Privacy Criteria Related to Monitoring and Enforcement.			
Trust Services Criteria: 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.			
P8.1.A	Internal and external users can report security and privacy related queries to privacyofficer@prophix.ca.	Inspected the intranet to determine whether internal and external users are notified to report security and privacy related queries to privacy.officer@prophix.com.	No exceptions noted.
P8.1.B	All emails to privacyofficer@prophix.ca are logged in the ticketing system for follow-up action based on pre-defined escalation criteria.	Inspected the privacy officer's inbox to determine whether privacy incidents were logged and follow-up actions had been performed.	No exceptions noted.