moengage

NOTE: You may not distribute this SOC 2 report for MoEngage to other parties, except where MoEngage is a component of the services you deliver to your customers. In this circumstance, you may distribute this SOC 2 report to current and prospective customers/users of your own services. You must provide recipients of this SOC 2 report written documentation of the function that MoEngage provides as it relates to your services. You must keep a complete and accurate record of entities and the personnel of such entities to whom this SOC 2 report is provided. You must promptly provide copies of such records to MoEngage or Accedere Inc upon request. You must display or deliver the language in this paragraph or language that is substantially equivalent to this paragraph to recipients of this SOC 2 report for MoEngage.

Attest Report by

MoEngage

SOC-2 Type 2 and CCM Report

Program:

Intelligent Customer Engagement Platform SaaS Application Services

Period Covered

June 1, 2022 to May 31, 2023

Table of Contents

Executive Summary

Scope	MoEngage's Intelligent Customer Engagement Platform SaaS Application Services
Period Covered	June 1, 2022 to May 31, 2023
Applicable Trust Services Criteria	Security, Availability, and Confidentiality
Additional Controls	Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Version 4.0.7
Location	San Francisco, USA Bengaluru, India
Report Status	Unqualified

Section-I
Independent Service Auditor's Report
for the Security, Availability, and Confidentiality Criteria, CCM Criteria

999, 18th Street, #3000
Denver, Colorado 80202
info@accedere.io
https://accedere.io

Independent Service Auditor's Report

To
MoEngage,
USA

Scope

We have examined MoEngage accompanying Description of Controls for the period June 1, 2022 to May 31, 2023 ("Description"), specifically for its Intelligent Customer Engagement Platform SaaS Application Services and the suitability of the design of controls to meet the controls for the criteria set forth in Trust Services Criteria, (TSC 2017) for Security, Availability, and Confidentiality aspects as applicable and as stated in the Description. We have also examined the suitability of the design and operating effectiveness of controls to meet the criteria set forth in the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) Version 4.0.7 control specifications ("CCM Criteria") for the period June 1, 2022 to May 31, 2023. The Description may indicate that certain complementary user controls that may be suitably designed and implemented at the user level for related controls to be considered suitably designed to achieve the related criteria. We have not evaluated the suitability of the design or operating effectiveness of such complementary user controls and Sub-Service Organization Controls.

MoEngage uses its facility at the following address:

Office Location	Address
San Francisco, USA	315 Montgomery Street, 10th floor, San Francisco, 94104, USA
Bengaluru, India	1st Floor, 315 Work Avenue, Salarpuria Tower II, 22, Hosur Road, Chikku Lakshmaiah Layout, Adugodi, Koramangala, Bengaluru, Karnataka 560034.

To provide Intelligent Customer Engagement Platform SaaS Application Services to its clients. MoEngage does not use any sub-service organization that provides information or support to its Intelligent Customer Engagement Platform SaaS Application Services. The Description includes only those criteria and related controls of MoEngage relating to their Intelligent Customer Engagement Platform SaaS Application Services.

MoEngage Responsibilities

MoEngage has provided the attached assertion titled Assertion of MoEngage (Management Assertion) about the fairness of the presentation of the Description and suitability of the design of the controls to achieve the related control objectives, for the criteria stated in the Description relating to its services.

MoEngage is responsible for:

- Preparing the Description and the Assertion.
- The completeness, accuracy, and method of presentation of both the Description and Assertion.
- Providing the services covered by the Description.
- Specifying the controls that meet the applicable Trust Services Criteria, CCM Criteria and stating them in the Description; and

- Designing, implementing, and documenting the controls to meet the applicable Trust Services Criteria and CCM Criteria.

MoEngage is also responsible for providing the Intelligent Customer Engagement Platform SaaS Application Services covered by the Description, specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls to achieve the related control objectives for the criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on:

- The fairness of the presentation of the Description is based on the description criteria set forth in the MoEngage's Intelligent Customer Engagement Platform SaaS Application Services.
- Suitability of the design of the controls to meet the applicable Trust Services Criteria and CCM Criteria based on our examination.
- Operating effectiveness of the controls.

We conducted our examination in accordance with attestation standards SSAE 18 established by the American Institute of Certified Public Accountants and CCM Criteria. Those standards require that we plan and perform our examination to obtain reasonable assurance, about whether in all material respects:

- The Description is fairly presented based on the description criteria and
- The controls were suitably designed and operated effectively to meet the applicable Trust Services Criteria and CCM Criteria, for the period June 1, 2022 to May 31, 2023.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable Trust Services Criteria of Security, Availability, and Confidentiality only. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operated effectively to meet the applicable Trust Services Criteria and CCM Criteria. Our procedures also included evaluation of those controls that we consider necessary to provide reasonable assurance that the applicable Trust Services Criteria and CCM Criteria were met. Our examination also included evaluating the overall presentation of the Description. We believe that the evidence obtained is enough and appropriate to provide a reasonable basis for our opinion.

We did perform our procedures regarding the operating effectiveness of the controls stated in the Description and, accordingly, express an opinion thereon. We do not take any responsibility for MoEngage's Cyber Risk Management Program.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable Trust Services Criteria and CCM Criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design of the controls to meet the applicable Trust Services Criteria and CCM Criteria is subject to risks that the system may change or that controls at a service organization may become inadequate or fail. Cybersecurity risks are prevalent, malicious insiders or external third parties may be able to circumvent the controls at the service organization and may not be able to prevent such risks. Our examination or opinion does not cover such risks.

Opinion

In our opinion, in all material respects, based on the description criteria identified in the Assertion of MoEngage and the applicable Trust Services Criteria of Security, Availability, and Confidentiality and CCM Criteria:

- The Description fairly presents the controls that were designed and implemented for the period June 1, 2022 to May 31, 2023.
- The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable Trust Services Criteria and CCM Criteria would be met if the controls operated effectively for the period June 1, 2022 to May 31, 2023, and user entities applied the complementary user entity controls for the period June 1, 2022 to May 31, 2023.
- The controls tested, if operating effectively, were those necessary to provide reasonable assurance that the applicable Trust Services Criteria and CCM Criteria were met, operated effectively throughout the period June 1, 2022 to May 31, 2023.

Restricted Use

This report and the Description of Controls are intended solely for the information and use of MoEngage user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have enough knowledge and understanding of the following:

- The nature of the Intelligent Customer Engagement Platform SaaS Application Services provided by MoEngage.
- How the MoEngage's Intelligent Customer Engagement Platform SaaS Application Services system interacts with user entities or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at MoEngage to meet the applicable Trust Services Criteria.
- The applicable Trust Services Criteria and CCM Criteria.
- The risks that may threaten the achievement of the applicable Trust Services Criteria and CCM Criteria and how controls address those risks.

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

Accedere Inc.
Certified Public Accountants
CPA License No: FRM 5000337
Denver, Colorado, USA
Place of Issue: Denver, CO
Date: June 26, 2023

Stamp & Signature
Ashwin Chaudhary
MBA, CPA, CITP, CISSP, CISA, CISM, CRISC,
CGEIT, CDPSE, CCSK, ISO 27001LA, PMP.
info@accedere.io
https://accedere.io

Section-II
Management Assertion

moengage

Management Assertion

We have prepared the attached "Description of Controls" (Description) for MoEngage's Intelligent Customer Engagement Platform SaaS Application Services for the period June 1, 2022 to May 31, 2023, based on the criteria in items (a) – (c) below, which are the criteria for a description of a service organization's system("Description") in AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) (Description). The Description is intended to provide users with information about MoEngage's Intelligent Customer Engagement Platform SaaS Application Services intended to meet the criteria for the Security, Availability, and Confidentiality only (applicable Trust Services Criteria) set forth in Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP Section 100, AICPA, Trust Services Criteria 2017) and the criteria set forth in the CSA Cloud Controls Matrix (CCM) Version 4.0.7 control specifications (CCM Criteria). We confirm, to the best of our knowledge and belief, that,

a. The Description fairly represents the MoEngage controls for the period June 1, 2022 to May 31, 2023, based on the following description criteria:

   i. The Description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are as follows:
         (a) *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks)
         (b) *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)
         (c) *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers)
         (d) *Procedures.* Automated and manual procedures
         (e) *Data.* Transaction streams, files, databases, tables, and output are used or processed by the system

      (3) The boundaries or aspects of the system covered by the Description.

      (4) How the System captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities and other parties.

      (6) If the information is provided to or received from sub-service organizations or other parties.
         (a) How such information is provided or received and the role of the subservice organization and other parties
         (b) The procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

(7) The applicable Trust Services Criteria, CCM Criteria and the related controls designed to meet those criteria, including, as applicable, Complementary user entity controls contemplated in the design of MoEngage controls.

(8) If the service organizations present, the subservice organization using the carve-out method –
   (a) The nature of the services provided by the subservice organization
   (b) Each of the applicable Trust Services Criteria and CCM Criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria
   (c) MoEngage confirms that it does not use any sub-service organizations for its services

(9) Any applicable Trust Services Criteria and CCM Criteria that are not addressed by MoEngage controls and the reasons.

(10) Other aspects of our control environment, risk assessment process, information and communication systems, control activities, and monitoring controls that are relevant to the services provided to user entities of the system.

(11) Relevant details of changes to the MoEngage system during the period covered by the Description.

ii. The Description does not omit or distort information relevant to the MoEngage system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the Description were suitably designed throughout the period June 1, 2022 to May 31, 2023, to meet the applicable Trust Services Criteria and CCM Criteria.

c. The controls stated in the Description operated effectively throughout the period June 1, 2022 to May 31, 2023, to meet the applicable Trust Services Criteria and CCM Criteria.

For MoEngage

Sd/-
Name: Nitin Kotwal
Designation: Head of Security
Date: June 26, 2023

Section-III
Description of Controls
Provided by Intelligent Customer Engagement Platform SaaS Application Services of MoEngage

Description of Controls provided by MoEngage

Services Provided

DC1: The nature of the MoEngage's business and operations, including the principal products or services MoEngage sells or provides and the methods by which they have distributed.

Background

- MoEngage Inc. (hereinafter referred to as MoEngage) is headquartered in San Francisco, USA with a back-end operations office in Bengaluru, India was incorporated in 2014 by Raviteja Dodda and Yashwanth Kumar, both alumni of IIT Kharagpur.
- MoEngage's business objective is to make orchestrating moments-based customer journeys a reality. MoEngage helps clients analyze end-customer behavior and then act on insights with personalized messaging to the end-customers preferred channel, at the right time.
- With the vision to build the world's most trusted customer engagement platform, MoEngage has been recognized as a Customers' Choice vendor in the 2022 Gartner Peer Insights' Voice of the Customer': Multichannel Marketing Hubs Report and is the youngest company on the report, with an overall rating of 4.8. MoEngage is also recognized in The 2022 Gartner® Magic Quadrant™ for Multichannel Marketing Hubs, and is also featured in G2 Spring 2023 Grid® Report as Mobile Marketing and Analytics Industry Leader.

Overview of Service

- MoEngage provides an intelligent customer engagement platform, built for the mobile-first world with AI-powered automation, optimization capabilities, and in-built analytics. MoEngage enables hyper-personalization at scale across multiple channels like mobile push, email, in-app, web push and SMS.
- With a mission to support digital engagement and growth for user-centric brands from e-commerce, retail, travel and hospitality, banking and financial services, media and entertainment, telecom, food delivery, and mobility verticals; MoEngage serves Fortune 500 brands across 39+ countries.
- We help our clients develop and launch products that increase revenue, and improve profitability, thereby driving top and bottom-line growth. By using our solutions our clients build innovation capabilities, leverage new technologies, and nimbly adjust to changing business demands by extending their capabilities with access to highly competent talent.

AWS Organization

MoEngage utilizes Amazon Web Services, AWS, taking advantage of several key AWS services, including Amazon Elastic Compute Cloud (Amazon EC2). MoEngage also utilizes MoEngage Kavach and Deepfence hosted on AWS IaaS for securing MoEngage SaaS Infrastructure config and data plane components including Amazon EC2 instances.

Boundaries of the System

The boundary of the system is restricted to provide application support services to MoEngage Intelligent Customer Engagement Platform provided as a software-as-a-service.

MoEngage Inc's description of service includes a Description of MoEngage India's application support services used by it to process transactions. The controls at MoEngage India have been designed by MoEngage Inc and are implemented and operated by MoEngage India, to the extent they are necessary for MoEngage Inc to achieve its service commitments and system requirements.

The specific services included in the scope are the development and maintenance of MoEngage products, establishing business processes in various departments, monitoring compliance, etc. supported from the Location in Bengaluru, India.

All material activities and operations relating to MoEngage software development are performed in Bengaluru, India. No customer data is stored on the MoEngage office network unless otherwise authorized by the customer.

MoEngage IT teams connect to VPN to manage the deployed solutions.

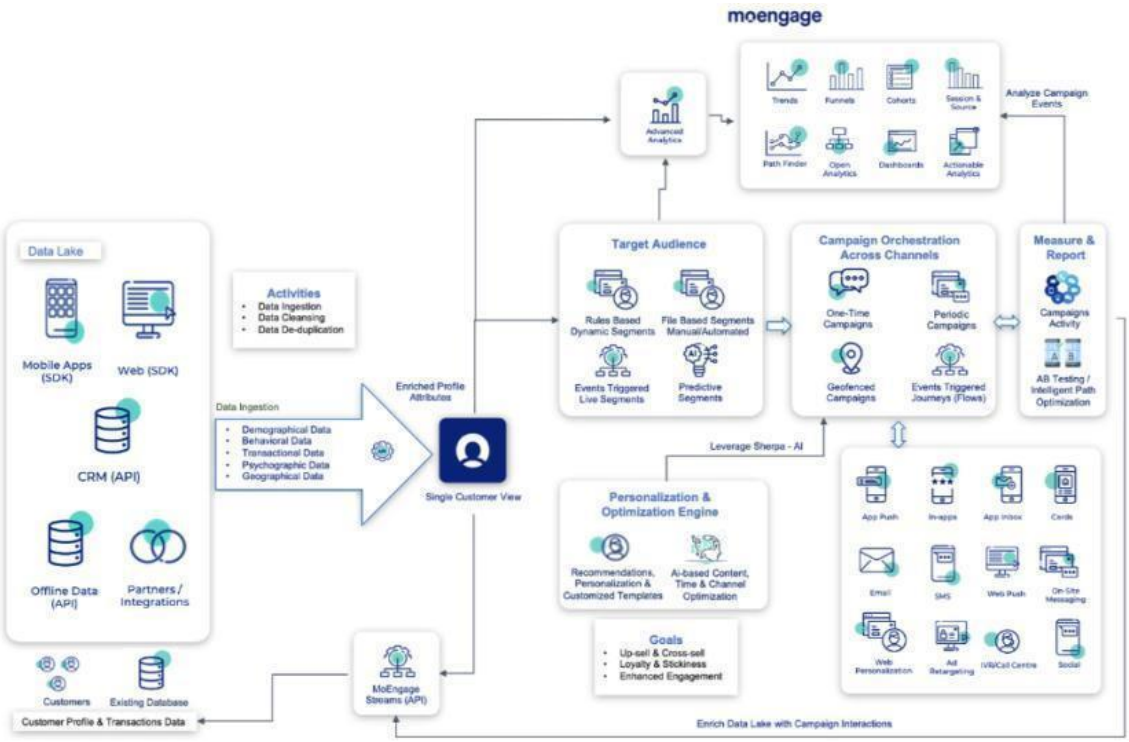
Geographic locations covered by the report include the Development Centre in Bengaluru, India, and Headquarters level operations in San Francisco, USA.

Registered Entity	Office Location	Address
MoEngage Inc	San Francisco, USA	315 Montgomery Street, 10th floor, San Francisco, 94104, USA
MoEngage India Private Limited	Bengaluru, India	1st Floor, 315 Work Avenue, Salarpuria Tower II, 22, Hosur Road, Chikku Lakshmaiah Layout, Adugodi, Koramangala, Bengaluru, Karnataka 560034.

For the reader's convenience, both organizations, namely MoEngage Inc and MoEngage India are collectively known as MoEngage in the remaining part of this Section 3 unless separately required to be stated so. The report excludes all processes and activities that are executed outside India and US in respect to MoEngage Business Process.

MoEngage SaaS Application Overview

MoEngage is an integrated platform that enables consumer brands to use real-time and contextual insights to engage with users across channels.



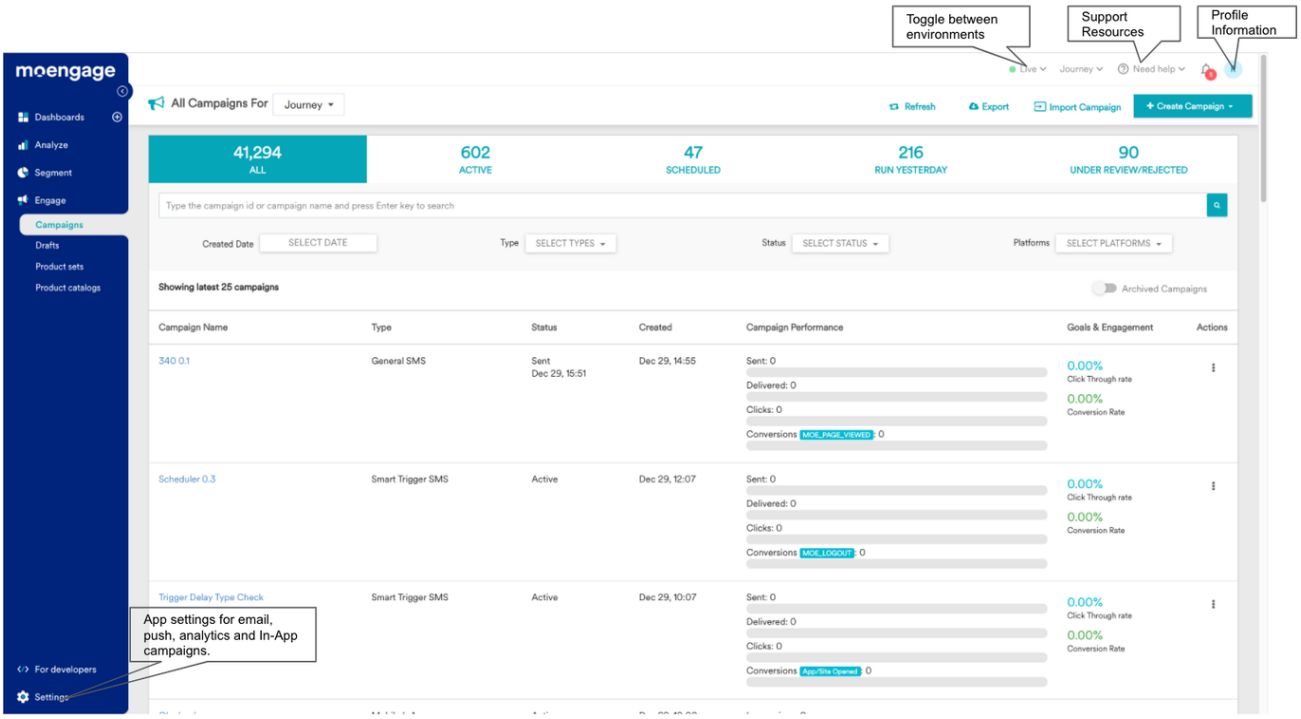
a. SaaS Application Hosting Data Centers

MoEngage maintains multiple data centers, used to host SaaS Infrastructures based on customers' regional & industrial compliance and performance requirements. Based on the data center the dashboard, SDK, and REST API gateways are provided to the customer.

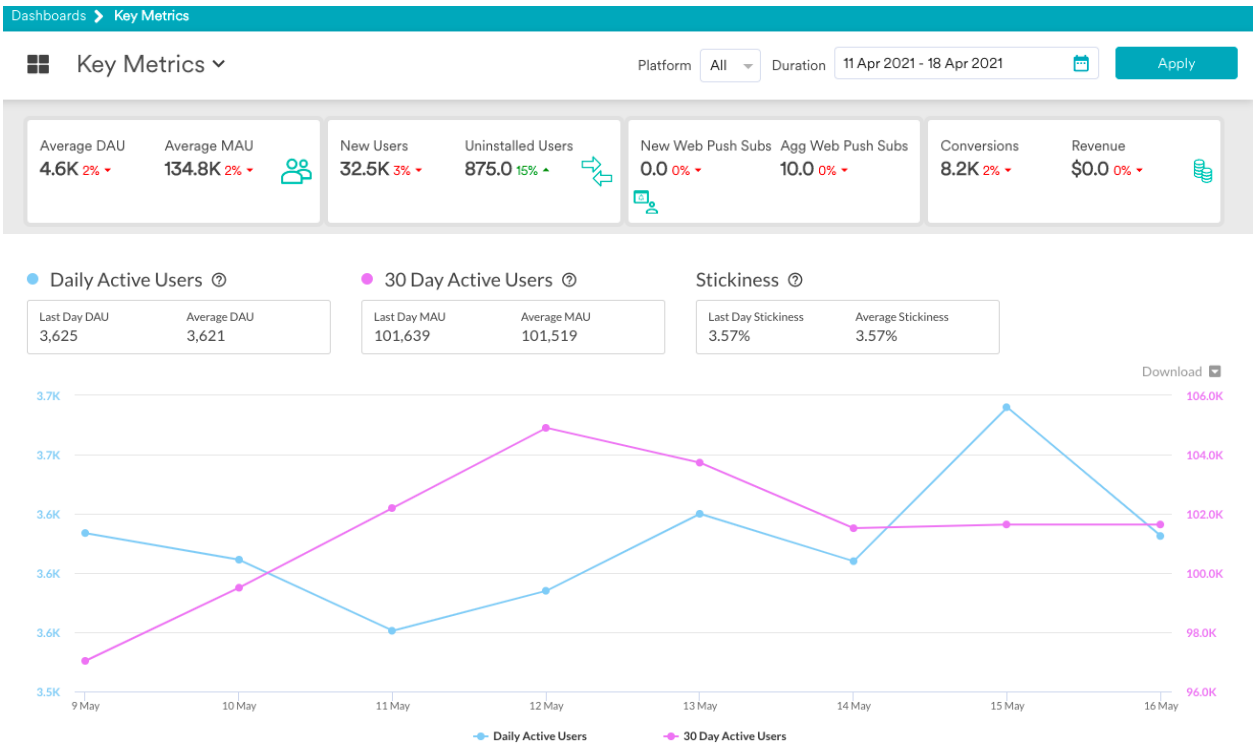
Cloud Data Center(DC) Name	Cloud DC Location	Dashboard URL	REST API Host
DC-01	North Virginia, US	https://dashboard-01.moengage.com	https://api-01.moengage.com
DC-02	Frankfurt, Germany	https://dashboard-02.moengage.com	https://api-02.moengage.com
DC-03	Mumbai, India	https://dashboard-03.moengage.com	https://api-03.moengage.com
DC-04	Ohio, US	https://dashboard-04.moengage.com	https://api-04.moengage.com
DC-05	Singapore	https://dashboard-05.moengage.com	https://api-05.moengage.com

b. SaaS Application Dashboard

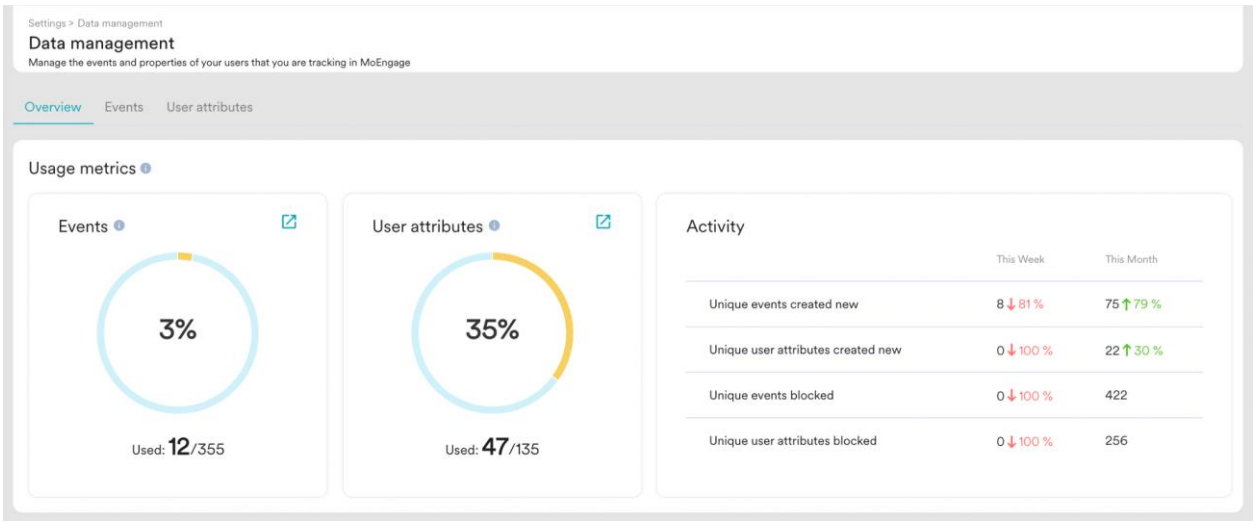
MoEngage Dashboard provides quick access to all MoEngage features including analytics, segmentation and campaigns.



Key Metrics is a dashboard page that provides all the important & necessary information for day-to-day use for marketers. A quick glance at Key metrics shows the usage, engagement, and performance metrics of the product.

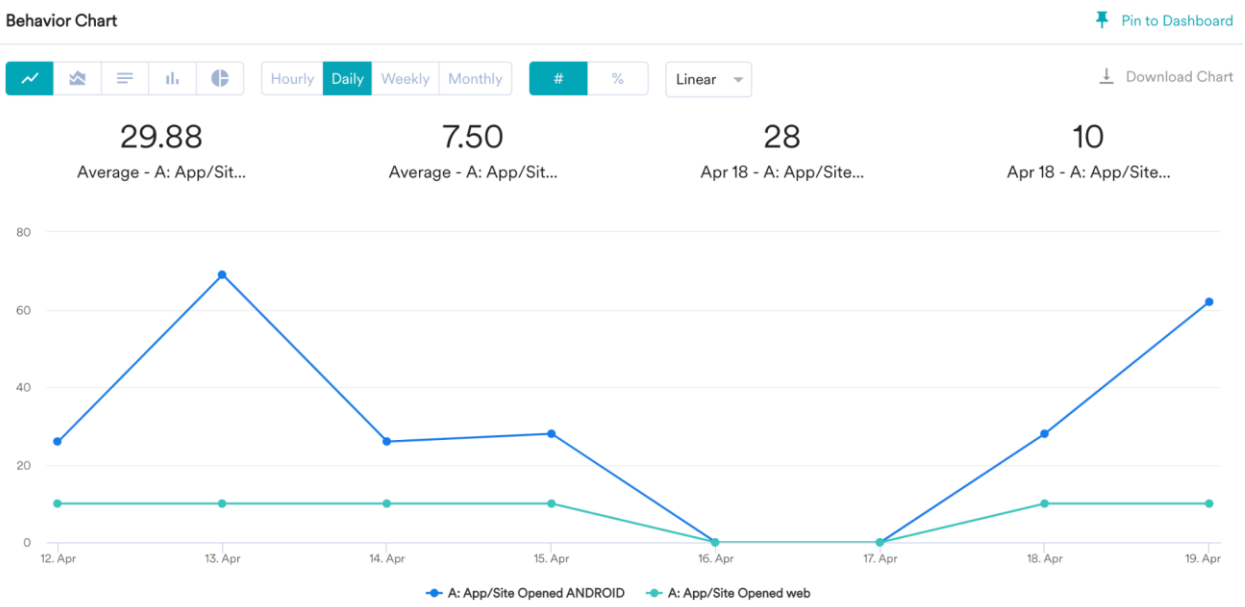


MoEngage Data Management features allow effective management of events and user attributes to ensure customer marketing efforts through MoEngage are optimized and prone to fewer errors.

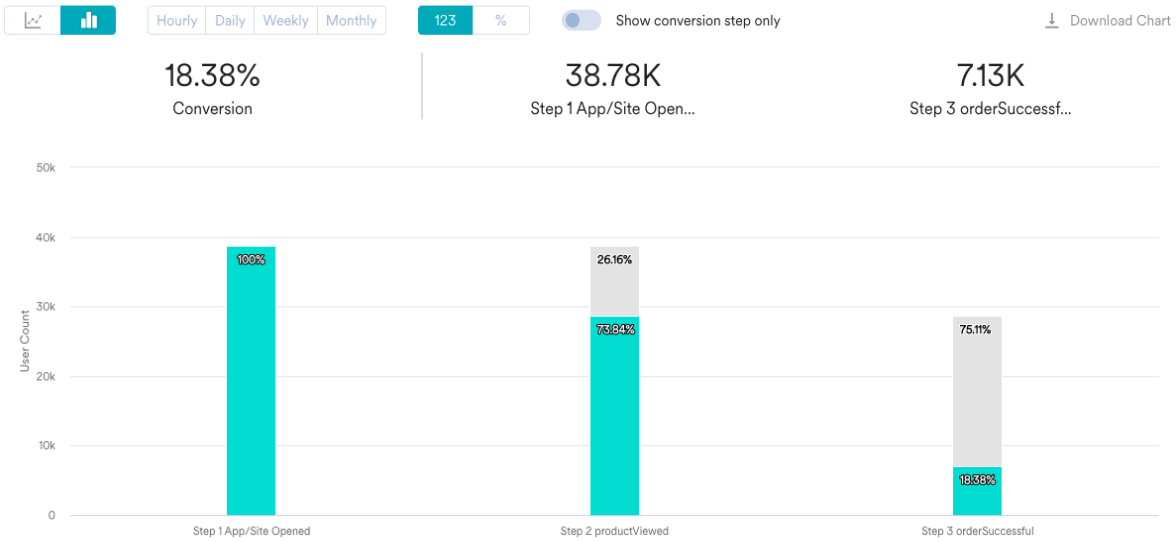


c. Analytics

- Behavior Module in MoEngage Analytics helps to understand how MoEngage Customer's end users interact with their web and mobile apps. We drill down the analysis for tracking events and analyzing trends of the app and campaign performance.



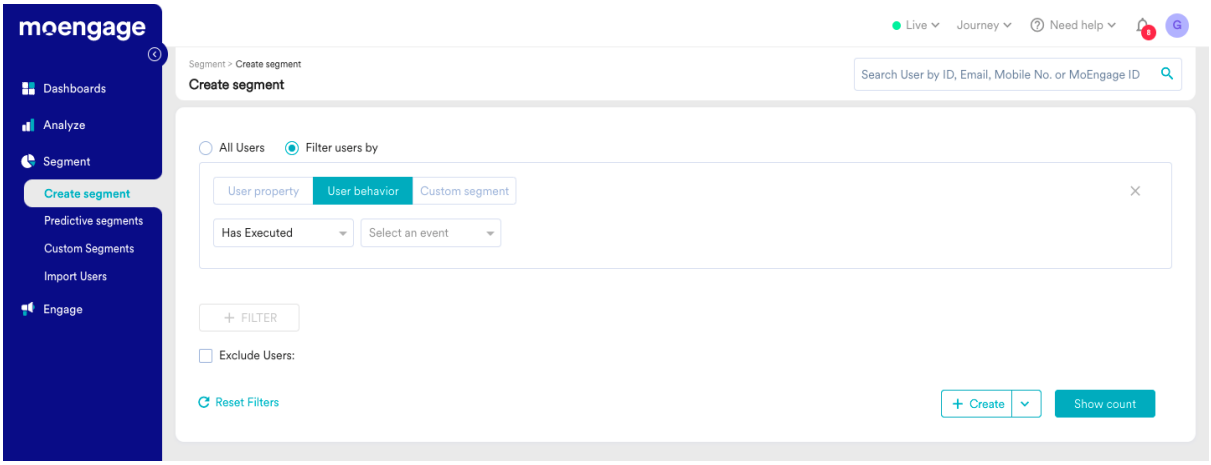
- A Funnel is a series of events that lead to a predefined goal event. Funnel analysis is primarily used to calculate conversion on specific user behaviors.



- The Cohort module of MoEngage Analytics helps to understand user cohorts & retention, essential to understanding product health with respect to loyal returning users. A cohort is a set of users, who are identified by their common behavior. The cohort for web and app analytics is a group of users who have performed the same events in a given duration.

d. Segmentation

A segment is a group of users defined by specific properties or values. Segments are used to send campaigns or to analyze specific information or behavioral traits of users.



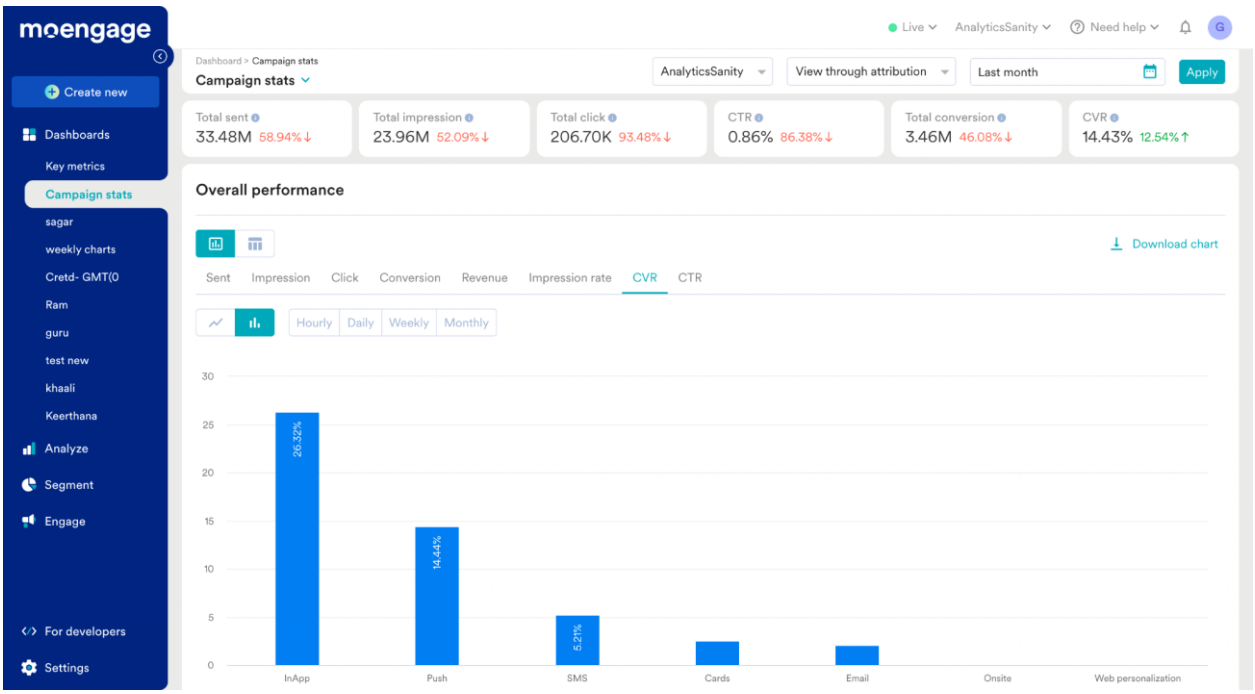
e. Campaigns and Channels

Channels, in the MoEngage SaaS services context, are defined as a medium to deliver the message or other actions. MoEngage supports multiple channels to help marketers and Product owners engage their audience across relevant and important touch-points.

Currently, MoEngage supports channels as below:

Channel Name	Channel Description
Push (App)	Used to send out a push notification on devices having your Mobile (Android, iOS) apps installed
Web Push	Used to send out a push notification to your Desktop & Mobile websites on supported browsers
Email	Used to send out an email to an end user
SMS	Used to send out a SMS to an end user
In-app	Used to display messages inside your mobile app when users are using the app
On-site	Used to display pop-up messages/survey or generate leads inside your Desktop or mobile website when users are using the website
Cards	Used to display the messages inside a feed which can be embedded inside your app
WhatsApp	Used to send templated WhatsApp Messages to end users who opted-in for WhatsApp
Facebook Audience	Used to retarget users on Facebook by syncing data to Facebook Ad Audience
Connectors	Used to integrate and send data to any other channel/partner or 3rd party tool to which you wish to forward the data or trigger communication
Web Personalization	Used to personalize the experience of end users when they come and use your website

Campaign stats provides a single dashboard view of all the campaigns in all the channels to provide an overview of all executed campaigns and displays analysis data across or specific channels.



f. **PII Masking**
g. **PII Data Encryption**
h. **PII Tokenization Sending**

Principal Service Commitments and System Requirements

DC2: The Principal Service commitment is to provide SaaS Application Services to MoEngage customers reliably.

Security at MoEngage

MoEngage takes data security, privacy, and compliance very seriously. We have put in several standards and diligently follow protocols to protect our customer's user data. MoEngage follows a "security by design" philosophy. This means MoEngage does not treat security as an afterthought. The "security by design" team consists of product managers, architects, engineers, and compliance consultants, who review privacy policies and security measures regularly.

MoEngage is committed to abiding by increased transparency regarding the collection and processing of personal information.

Confidentiality

MoEngage gives high priority to customer information confidentiality. MoEngage ensures

- Data Encryption at Rest by enabling AES-256-GCM encryption across all our Data volumes where customers' Personal Data resides.
- Data Encryption in Transit by utilizing TLS 1.2 encrypted Channel for all Public-facing interfaces.

Integrity

Along with confidentiality, MoEngage also considers protecting the integrity of the data both in transmission and at rest. Utilization of JSON Web Tokens [JWT] with signatures, Strict Role-based access Controls across SaaS Infrastructure, Private Network for SaaS Infrastructure, Monitoring, Approval, and Auditing for all Production changes, Utilization of required End-point Security Controls ensures Data Integrity of stored Customer's Personal Data.

Availability

MoEngage ensures annual availability of 99.9% for all MoEngage services and applications to help the customers utilize the platform to the highest and make use of redundant resources to make sure the services are available to MoEngage customers without any interruptions. MoEngage takes continuous backups and follows a disaster recovery plan to ensure the MoEngage platform is available even in case of unexpected scenarios.

Authentication

Utilization of Federated login [SAML 2.0] and Two Factor Authentication, Complex Passwords, Account Lockout policy and Regular Audits to ensure secure access across Organization.

Authorization

MoEngage ensures the Principle of Least Privilege, No Default Access, Granular and Auditable Role-based Access Controls for any access to SaaS Infrastructure. Any access to a Customer's Personal Data requires auditable approval from the Customer.

Accountability

MoEngage ensures the generation and continuous monitoring of auditable log trails. All Configuration changes along with Database activities are strictly monitored and audited on a time-to-time basis.

A few of the key practices MoEngage follows under the Security Process:

- Implementation of CERT DevSecOps model to ensure Secure Development and Deployment of any application
- In-depth VAPT (vulnerability assessment and penetration testing) for any application going into production.
- Regular assessments of all our infrastructure on a quarterly basis.
- Continuous audits on all our database machines to ensure high-security standards.
- AES-256 encryption for all our data volumes.
- Regular info-sec assessments on all MoEngage Corp assets to ensure security at the End Point level.
- Support for SSO via SAML 2.0 and act as a service provider (SP) for SSO.
- Compliance with multiple privacy regulations like California Consumers Protection Act (CCPA) along with GDPR
- RBAC for all MoEngage internal application/software(s) to ensure only authorized personnel perform privileged actions.

MoEngage SaaS Service Delivery Teams

a. **Security Office (**hereinafter referred Security Team**)**

This team has a primary responsibility to ensure,

- System Integrity and Confidentiality requirements
- Config and Data plane Security Monitoring
- Change and Patch management
- Network and System Hardening
- Incident management in MoEngage
- Access Control

- Vulnerability Assessment/Penetration Testing
- Internal Audit
- Antivirus updates and control
- Security Compliance and Regulation Management

b. Engineering (Software Development) Team

Engineering team is responsible for the Software Development [product] aligned with MoEngage SDLC. The main responsibility includes:

- Product Requirement Development (PRD Template), (Requirement Phase)
- Technical Architecture (Tech Doc Template), (Design Phase)
- Product Development activities (Coding Phase)
- Product Testing (QA/Testing Phase)

c. Site Reliability Engineering (SRE) Team

SRE team is responsible for the stability and performance of SaaS Infrastructure. Key responsibility includes SaaS Infrastructure

- Configuration & Deployment
- Automation
- Stability and resilience assurance
- Performance, monitoring

d. People and Culture (HR) Team:

HR team governs the work environment and promotes ethics and integrity. The main responsibilities include

- Recruitment
- Onboarding of employees
- Learning and Development
- Background checks
- Severance on resignation or termination
- Performance evaluations including cases of non-performance
- Rewards and incentives
- Analyzing the cases of disgruntled employees and possibilities of frauds

e. Finance and Legal Team

Finance and Legal team govern the accounting and legal practices for both Indian and US entities. The main responsibilities include:

- Employee Compensation
- Financial and legal compliances
- Procurement and Supplier Relationship
- Budgeting and Planning
- Legal Services co-ordination
- Company Secretarial services for the board

f. Sales and Marketing Team

Sales and Marketing are two separate and independent functions. The activities in these functions are Sales Development, Market Research, Customer Discovery and Education.

g. Customer Success Management [CSM]

The activities in the CSM team includes Sales-handover, Customer Onboarding, Success Management, and Customer Off-boarding.

Key infrastructure components include the following:

- **Amazon Web Services (AWS) platform**
  Key AWS services, including Amazon Elastic Compute Cloud (Amazon EC2), S3, ELB, EBS, CloudTrail, Elastic Search etc. Continuous monitoring of AWS services is ensured by the SRE team.
- **Data Plane Monitoring**
  Deepfence is deployed as a Container-based Application Firewall for runtime monitoring and analyzing the traffic of known and behavior-based attack patterns. The appropriate security personnel are alerted when incidents are detected.
- **Config Plane Monitoring**
  MoEngage In-house developed “Kavach” tool is deployed for granular and continuous monitoring of configuration, change management, and audit of SaaS Infrastructure.
- **Access Management**
  StrongDM is deployed as a bastion host to ensure granular Access to each SaaS Infrastructure component. Access is monitored, audited, and recorded for forensics analysis.

Components of the System used to provide the Services

DC3: The components of System Framework that coexist to support MoEngage's business operations including infrastructure, software, people, procedures, and data.

AWS Platform

MoEngage Systems utilizes third-party hosting providers (Amazon Web Services, AWS) separately for production and development environments.

MoEngage takes advantage of several key AWS services, including Amazon Elastic Compute Cloud (Amazon EC2), S3, EBS, CloudWatch, CloudTrail, etc.

The infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources.
The cloud infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards.

Boundaries of the System

The infrastructure comprises physical and hardware components of the System including facilities, equipment, software and networks installed at AWS Cloud.

Hardware components of a system

MoEngage is equipped with the latest state-of-the-art infrastructure which enables the smooth execution of their projects. Its offices are equipped with the latest hardware, software and networking infrastructure. Offices are connected to the internet using highspeed communication links, backed up by redundant networks. Access control is governed by the access privilege policy.

All employees are provided with laptops, which are pre-installed with Mac OSX and anti-virus software. Based on the need, MS Office software is also provided. Trainees are provided with laptops or desktops which are also pre-installed with Mac OSX and anti-virus software. The software and hardware assets are logged in an asset register and maintained up to date by the IT team members.

MoEngage Cloud Infrastructure is equipped with the latest hardware, software, and networking controls. The infrastructure comprises physical and hardware components of the System including facilities, equipment, software and networks located at AWS Cloud Datacenters. The production infrastructure is monitored and managed 24x7 by SRE and Security Office.

The report excludes all processes and activities that are executed outside India and US in respect to MoEngage Business Process.

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.

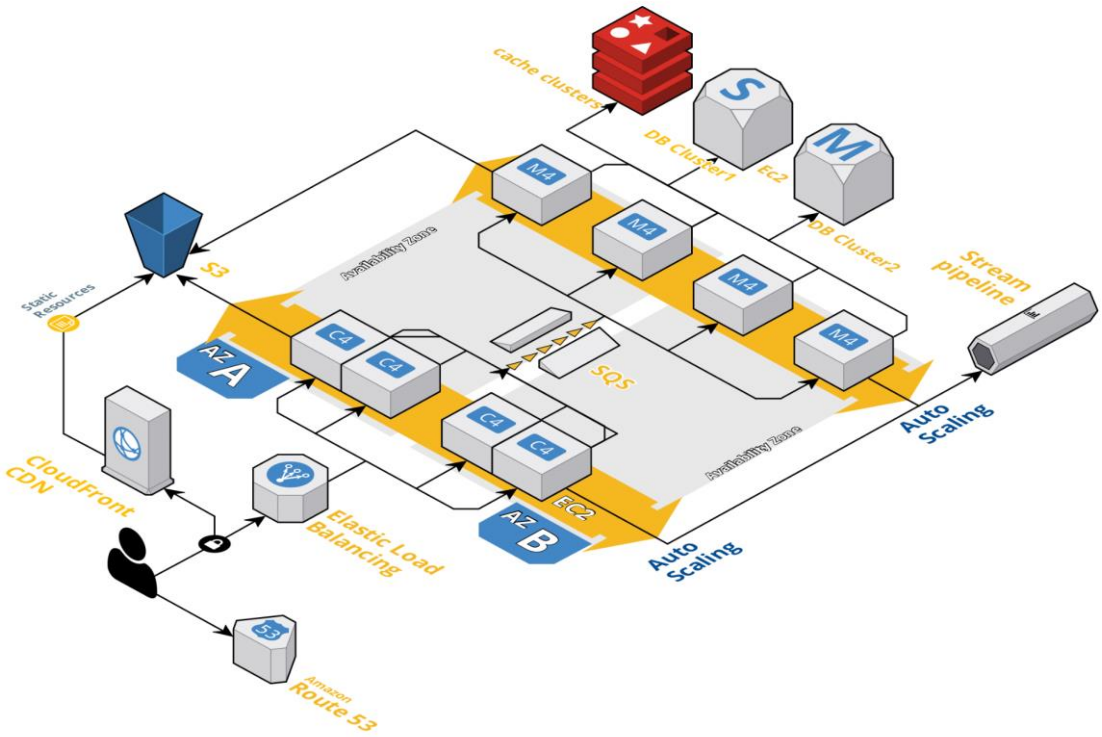
Processes, Policies and Procedures

Formal policies and procedures exist that describe logical access, information security, user data confidentiality, risk management and change management. All teams are expected to adhere to MoEngage's policies and procedures that define how services should be delivered.

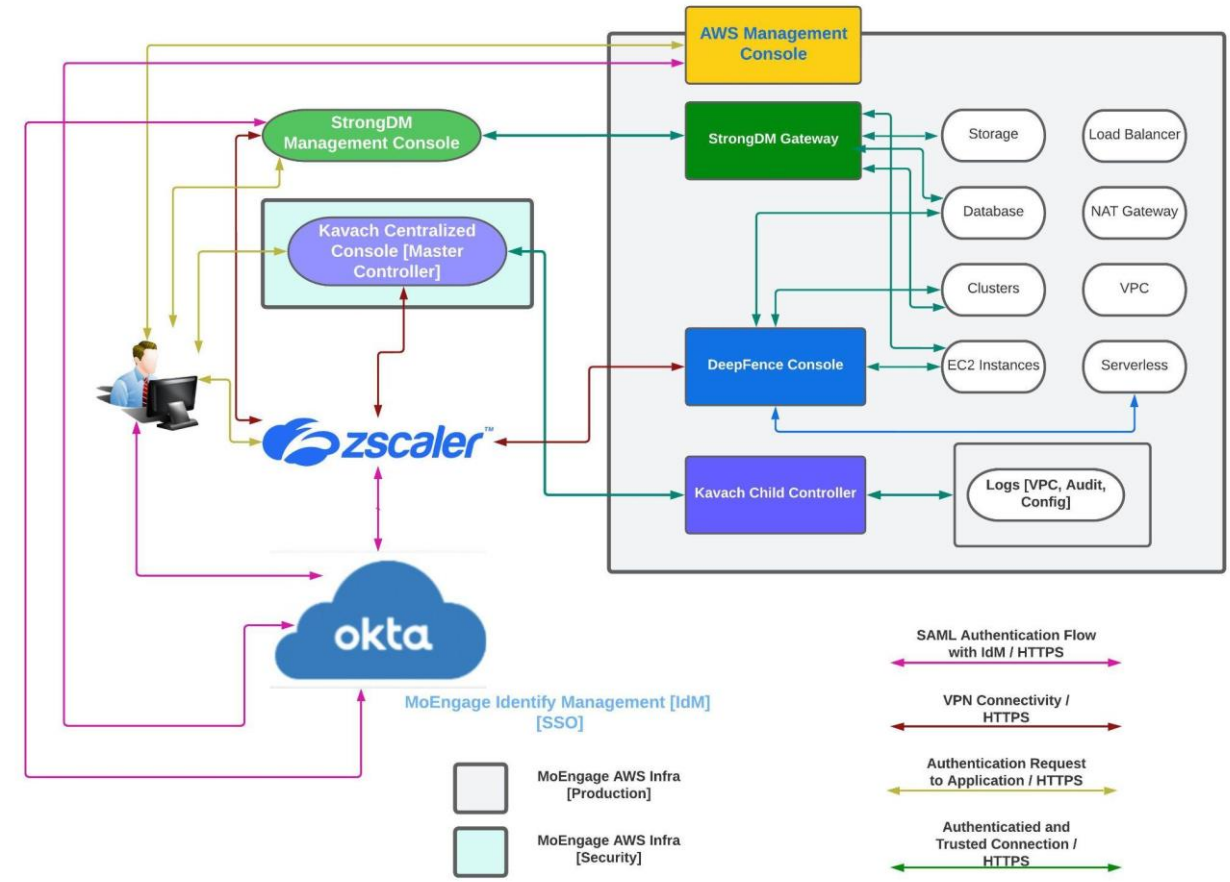
Stage & Prod Instance Segregation

There exists a dedicated and separate AWS Cloud environment for Stage and Production instances for customer applications. Developer access to the production environment is restricted. Change promotion to Production instance first goes through Stage.

SaaS Infrastructure Network Diagram



Utilized AWS Cloud Services/Components



SaaS Infrastructure Security Controls

AWS data center physical security Overview

MoEngage relies on AWS for the physical security of its SaaS Infrastructure.

a. Perimeter Layer

This Layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

b. Infrastructure Layer

This layer includes the data center building and the equipment and systems that keep it running. Components like backup power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer. These devices and systems help protect servers and ultimately your data.

c. Data Layer

The Data Layer is the most critical point of protection because it is the only area that holds MoEngage data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, AWS deploys threat detection devices, video surveillance and system protocols, further safeguarding this layer.

d. Environmental Layer

The Environmental Layer is dedicated to environmental considerations from site selection and construction to operations and sustainability. AWS carefully chooses data center locations to mitigate environmental risks, such as flooding, extreme weather, and seismic activity.

The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities are performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Regular Third-party testing of AWS data centers ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

Software

The list of the software and tools that are used to manage business requirements and control the environment at MoEngage.

Tools/Software	Purpose
Okta	Single SignOn Server
Google	Identity Management
Jamf	Mobile Device Management Solution for MacOS based devices
Microsoft Intune	Mobile Device Management Solution for Windows OS based devices
Sophos	Host based Antivirus solution
Tresorit	Secure File sharing Solution
Zoom	Hosting Virtual Meetings
Google Meet	Hosting Virtual Meetings
Lucidchart	Creating SaaS Infra and Application components Architecture
Microsoft Office Suite [Excel, Powerpoint, MS Word]	Business productivity tool
Atlassian [Jira, Confluence]	Ticketing / Knowledge base management
Cisco Meraki	Office Wireless Network management
Freshservice	IT Ticketing tool
Slack	Internal Communication Tool
Zscaler	Cloud based VPN Solution
OneTrust	Incident Management, PIA, DPIA Management and Tracking
Scrut	Compliance Management Tool
Burp Suite Professional	Manual Application Penetration Testing tools test
Burp Suite Enterprise Edition	Dynamic Application Security Testing
Checkmarx	Static Application Security Testing
AWS	Cloud Infrastructure hosting [IaaS]
StrongDM (SDM)	Cloud Based Access Monitoring system, Bastion Host

Tools/Software	Purpose
UpGuard	External Threat Identification Tool
Deepfence	NextGen Application Firewall, Intrusion Detection System and Endpoint Detection and Response
Kavach	MoEngage Internal Tool for Cloud configuration monitoring and auditing
HashiCorp Vault	MoEngage Internal Secret Management Tool
Harness	Security Pipeline and Deployment [CD]
Jenkins	MoEngage Internal CI/CD Tool
JFrog Artifactory	Release artifacts repository
Java, Python, Go Lang	SaaS Application Business logic development
Angular, HTML, CSS, JavaScript, jQuery	SaaS Application UI Development
Zendesk	Customer ticket Management tool
Vscode, Android studio, IntelliJ IDEA, Xcode, Pycharm CE	IDE for software development
GitHub	Source code repository
TLS 1.2	Encrypted communication channel
AWS Services - EC2, Kubernetes, S3, CloudWatch, CloudTrail, EFS, Security groups, VPC, etc.	SaaS Infra Hosting components
PagerDuty	Event Notification and Alerting
Sentry	Error tracking platform
Salesforce	Sales & Marketing team for managing prospects
Trakstar	Hiring portal
Darwinbox	Human Resource Management System, For Employee Tax & Salary information.
Snyk	Software Composite Analysis

People

Executive Leadership Team (ELT)

MoEngage's Executive Leadership Team (ELT) is committed to the development and implementation of the MoEngage Information Security Management System which is both compatible with the strategic direction and the context of the organization, the whole system is frequently reviewed to ensure conformance to industry standards and practices. Responsibility has been assigned to ensure that the business Management System conforms to the requirements of the respective standard and the provision to report on performance to the top management team has been defined.

The designated Leadership Representative(s) will ensure that MoEngage staff is aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving MoEngage's Information Security Policy and Objectives which are aligned with the organization's strategic direction.

The ELT is responsible for implementing this system and ensuring the system is understood and complied with at all levels of the organization.

ELT consists of the Board of Directors, VP, EVP and different department heads of India and US operations. includes the Information Security Team (InfoSec Team), collectively called the MoEngage InfoSec Steering Committee (ISC). ISC meets half-yearly to audit security controls, reports and roadmap.

ELT meets monthly to review MoEngage roadmap, strategies, financial statements, and adherence with regional compliance and regulation requirements.

Management's Philosophy and Operating Style

The Executive Leadership team at MoEngage assesses risks prior to venturing into business ventures and relationships. The size of MoEngage enables the ELT to interact with operating management daily.

Service processes

Project management & Customer communication teams are involved in the analysis of client requirements, coordinate with technical teams to propose the solution, obtain necessary approvals and confirmations from the client and manage delivery. The project management team manages and includes sub-teams for software development, software support, software testing, software security & quality control.

Service processes

- *Activities phase*
  This process is the model or framework to provide technical and non-technical activities to deliver a quality system that meets the business expectations and manages the decision-making progression.

- *Requirement & Planning phase*
  Requirement of the project is to analyze the needs of the scope and ensure the system meets the expectation. After the boundary of scope is set then the planning phase is to determine the solution resources, cost time, and benefits.

- *Assurance phase*
  Assurance refers to the planned and systematic way of monitoring the quality of the process which is followed to maintain the quality of the product. It is proactive and plays an important role in each phase of the life cycle.

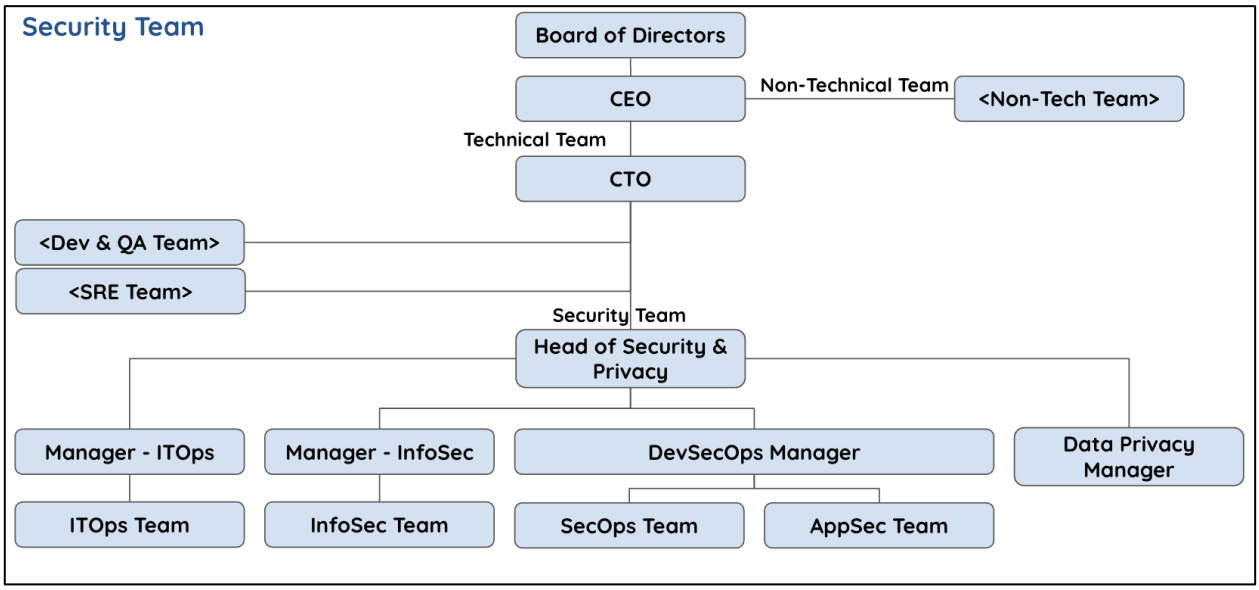
- *Support processes & activities*
  Support and maintenance activities involve maintenance and regular required updates. This step is when end users can fine-tune the system, if they wish, to boost performance, add new capabilities or meet additional user requirements.

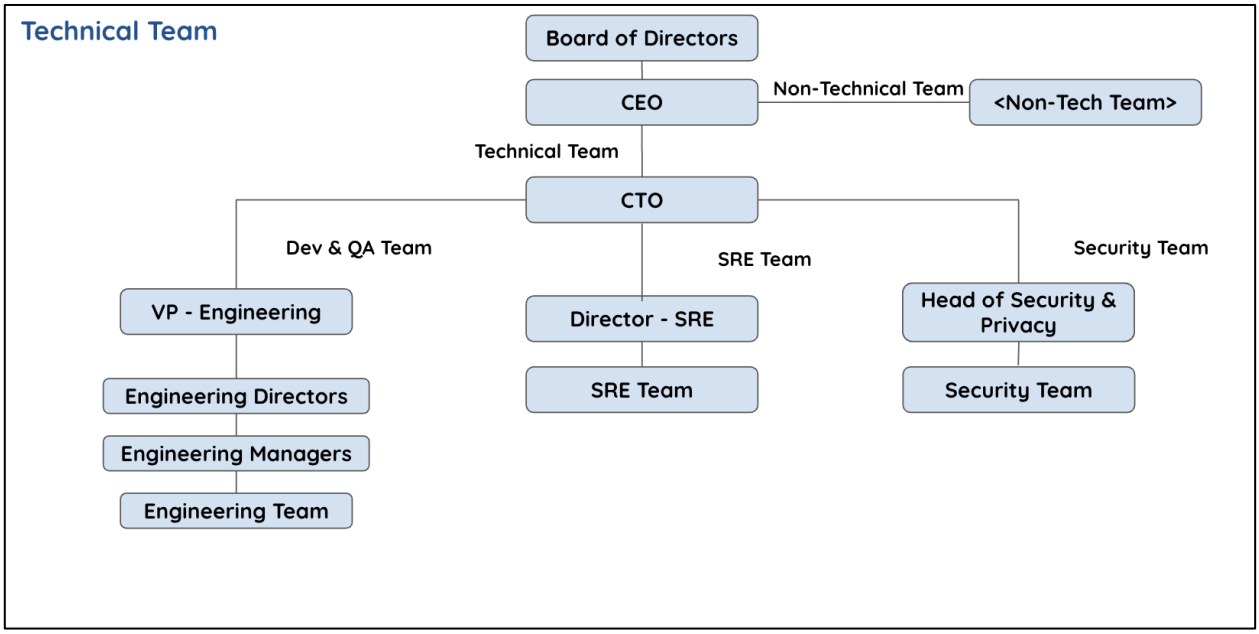
Organizational Structure

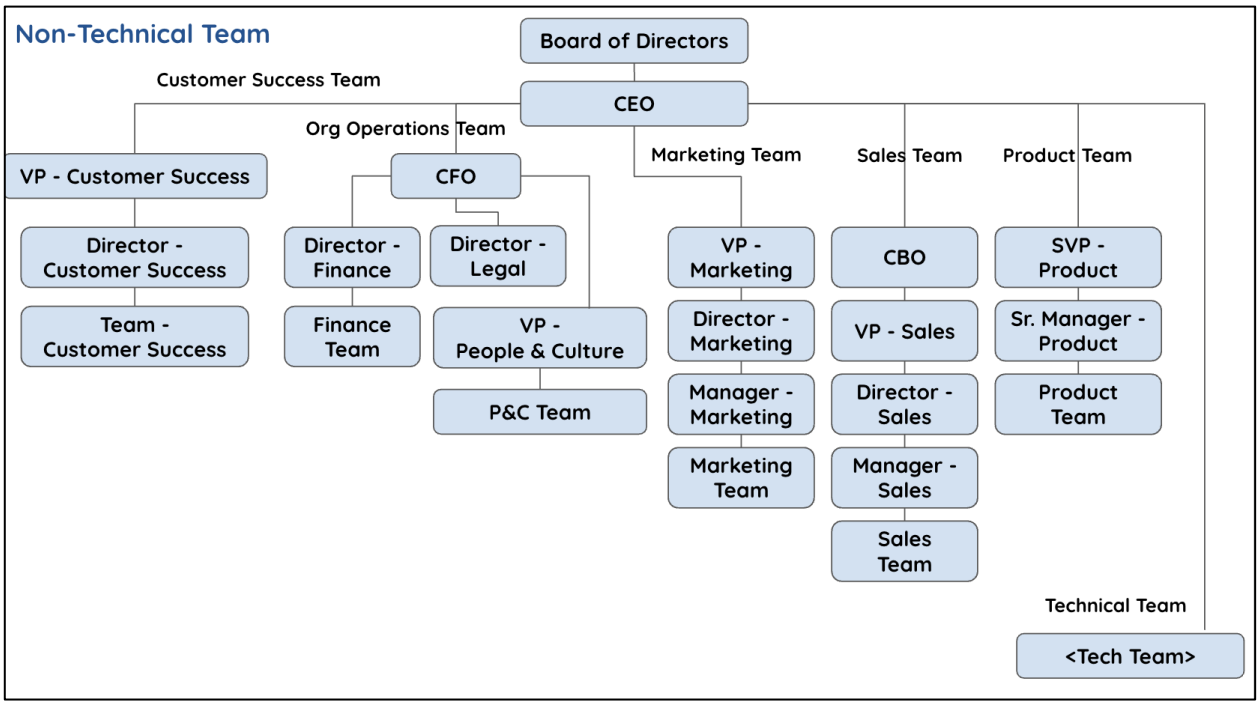
The organizational structure of MoEngage provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups per job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting MoEngage clients.

Written job descriptions for each role containing roles/responsibilities and job requirements in terms of skills, qualifications, and experience are reviewed by management and shared with HR whenever there is a job opening for that position. Job descriptions are provided to potential candidates so that they understand the job responsibilities.

MoEngage is organized in a functional reporting structure. Functionally, employees are managed within the Corporate Reporting Structure. MoEngage evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.


Security Team
Board of Directors
CEO
Non-Technical Team
<Non-Tech Team>
Technical Team
CTO
<Dev & QA Team>
<SRE Team>
Security Team
Head of Security & Privacy
Manager - ITOps
Manager - InfoSec
DevSecOps Manager
Data Privacy Manager
ITOps Team
InfoSec Team
SecOps Team
AppSec Team


Technical Team
Board of Directors
CEO
Non-Technical Team
<Non-Tech Team>
Technical Team
CTO
Dev & QA Team
SRE Team
Security Team
VP - Engineering
Director - SRE
Head of Security & Privacy
Engineering Directors
SRE Team
Security Team
Engineering Managers
Engineering Team



Corporate Reporting Structure

Company's Information Security policies define and assign responsibility/accountabilities for information security. The Head of Security and Security Team has custody of and is responsible for the day-to-day maintenance of the entity's security policies. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Procedures

New Hire Procedures

Recruitment is performed based on the request received from the Business Heads (Tech Operations). The required skill set and the Job description is shared by the Leadership and HR teams over email. Based on this input, suitable profiles / candidates are identified by the HR team for selection by the relevant business heads.

At the time of joining MoEngage, every employee is required to read MoEngage corporate policies and procedures and acknowledge them for adherence on HRMS portal, Darwinbox. Along with that, an employee needs to sign a set of forms including consent letter, acceptance to code of conduct, NDAs etc.

After hiring, candidates undergo background verification consisting of prior employer references and educational references. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination. All employees must sign an employment agreement with MoEngage containing code of conduct and commitments regarding security & confidentiality.

External consultants or third-party are evaluated before contracting. They are required to read and sign the contract, statement of work & NDA before commencing the assignment with MoEngage.

Once the employee has accepted the offer and then joins MoEngage, all the Organization level induction activities are performed by the HR team in coordination with the reporting supervisor / manager. Induction program covers company profile, policies, code of conduct, information security processes and practices. Attendance for these induction sessions is tracked by the HR team. After completion of the same, the employee is handed over to the business heads for functional induction.

Once the new employee joins the organization, the HR team sends an email to the Leadership, Functional and IT teams. Based on this email, the HR and Admin team grants access to the employee into the office premises. As required, the new employee's card and/or biometric inputs are captured and fed into the access control system to enable the employee to enter the office premises at any time.

Performance Evaluation

MoEngage has a performance review and evaluation program to recognize employees for performance and contributions. The MoEngage performance evaluation process is also used to help employees improve their performance and skill levels. Employees performance reviews, promotion, and compensation adjustment are performed every 12 months. The performance evaluation is reviewed with the employee.

Employee Exit Procedure

When the employee resigns, it is first communicated by the employee to his/her department head (functional supervisor) and the Head of HR. An exit form is completed by the employee to enable the HR group to initiate the 'Exit Process' to inform HR, Administration, IT support, Finance and Accounting teams for recording the last working day.

The process is then tracked at the HRMS portal and carried forward to the IT Operations team which de-activates/deletes the user ID from the domain followed by blocking of email access on the last day.

The HR team conducts an exit interview. Before the employee leaves, all the project related knowledge transfer is completed. The employee clearance form is signed by all the support functions to indicate that there are no pending activities to be done by the separating employee. The HR team sends an email to all the support functions. The Admin team revokes access to the office premises and the IT team revokes access to all the MoEngage's IT resources.

Change Management

The Change Management process describes a methodical approach to handle the changes that are to be made to its systems. All the changes are subjected to a formal Change Management process. The Change Management process at MoEngage covers system, IT infrastructure, network components. All major changes must be initiated by appropriate personnel, analyzed for impact, tested and approved before deployment.

Change requests pertaining to product features & modifications are recorded and tracked through the Jira system. All changes to the production system/application require the approval of the product manager for development to start. Any change is first tested in the local environment. On successful testing, the changes are migrated to the Stage environment.
If required, the customer SPOC is involved to verify the changes. After successful deployment on the Stage instance, the changes are promoted to the Production instance during the next available deployment schedule.

Any changes related to network or operating systems are also first tested locally for an adequate period before promoting to Stage, followed by the production environment. Critical patches are applied to priority. Non-critical patches are applied after seeking downtime from the customer. Rigorous testing of changes requires QA testing against dummy data, integration testing, Stage, etc. The testing strategy is devised by the company and test scenarios are maintained in Confluence.

Server Monitoring

The uptime of the MoEngage SaaS platform & health is constantly monitored through various services. The vital parameters of the servers like CPU, memory, disk usage & load average are monitored round the clock through monitoring scripts and monitoring tools. The scripts and tools trigger an email notification to MoEngage SRE and Security personnel if the threshold is crossed. The scripts also log the server status regularly. The logs are retained for an adequate duration and can be used to diagnose past issues.

Customer Onboarding

When a customer is signed-up, a detailed implementation plan is created after signing the contract and statement of work by both the parties. The implementation plan consists of the procedures that are used in the setup and ongoing plan administration. MoEngage manages the setups for new clients in such a way that activities for new clients are defined, assigned, tracked and completed as per the agreed project plan. The tasks, assignments, and dates for each onboarding are enlisted. Standard data templates are used if data is to be requested from the customer. The data migration in the system has validation checks so that data transfer is completed accurately, integrity is preserved, and any errors are identified. Each stage in transition, from Dev to QA to Prod goes through a test plan. The client signoff for data migration, Stage and go live are enlisted in the plan as milestones. MoEngage also manages customer issues and setups as part of the post-go-live operation processes.

Product Development Lifecycle

MoEngage follows the Agile methodology for product development lifecycle. The sprint cycle ranges from two to three weeks. A yearly product roadmap is defined by the Product Owner based on customer requirements and market demand. The features from the product roadmap are distributed into four quarters and picked up based on defined priority. The User Stories are entered in Jira and taken up based on priority. The Sprint progress for user stories is regularly updated and monitored in Jira. MoEngage development team uses standard software development tools to enable end-to-end product development lifecycle. The tools include different IDE, GitHub version control system, Jenkins for automated build, Checkmarx for SAST, Burp Suite Enterprise for DAST, Snyk for Software Composite Analysis, CodePipeline for automated deployment, Jira for defect tracking and user story management, and Confluence for test case management. Before the Sprint release, the product demo is presented to the product owner to ensure the acceptance criteria & product quality are achieved. After a successful demo, the development team sends a formal release mail to the Quality Check team to initiate testing. The Quality Check team will test the stories and test scenarios and certify the release if no blockers or critical issues are open. One build in each sprint is promoted to Stage, followed by the Production environment.

Release Management

MoEngage release management process begins with Sprint planning. The Spring planning meeting is held between the Product Management Group (PMG), QA Team, Development Team, and UI Team. At the end of this meeting, the User Stories are planned for Sprint. At the end of Sprint, a demo of all User Stories included in the Sprint is given to QA and PMG team. After a successful demo, the Sprint is released to the QA team. On successful release, the source code in the repository is tagged and branched by the release number. Any defects reported by the QA team in the given release are fixed in the branch as well as the trunk. Dev to QA release happens via Jenkins and build promotion is handled in Artifactory. QA team deploys the release on QA setups via automated deployment script. The deployment script is triggered through Jenkins. QA will perform the testing and certification in the stipulated time-period. One build per sprint is promoted to Sandbox (SB), Stage & Production environment in successions. The build promotion from SB to Stage to PROD happens through Artifactory. The deployment on SB, Stage, and PROD is carried via an automated deployment script triggered through Jenkins. When a new Release is upgraded on SB and/or Stage setup, the customer is informed about it by sharing the Release Notes.

The upgrade is followed by a cool-down period of one to two weeks. During this span, the customer SPOCs use the new features and report issues, if any. After addressing the issues, PROD upgrade is carried out. Apart from application upgrade, application patches also follow the above process. The upgrades on customer setups are performed during non-business hours of customers after informing the customers of the downtime window. This communication with the customer happens via Zendesk.

Patch Management

The Security, SRE and Development teams ensure that all patches to network device/servers operating systems are checked for stability & any availability; issues are tested before applying to the production environment.

All the critical & security patches are applied on a priority basis.

Virus Detection

Anti-virus software has been installed on all servers & laptops within the scope of MoEngage local and SaaS Infrastructure network. Updates to the virus definition files are managed and downloaded by the software itself daily from the vendor website every four hours. The antivirus server is managed remotely and configured to “Push” the latest signature updates to all systems on the network within the next four hours. If required, the rollback signature update can be done. Employees report any virus incident to the IT Operations team as part of the incident management process. Intrusion Prevention System (IPS) is enabled along with Antivirus which takes care of Network Intrusion Prevention and Browser Intrusion Prevention for Laptops.

Data

Data Backup and Restoration

On AWS Production Environment:
MoEngage has developed formal policies and procedures relating to back up and recovery. MoEngage production applications & databases are backed up at every twelve hours and last 30 days backups are retained. The backup scripts log the details of data being backed up for future reference. The backup scripts send a daily notification indicating the status of the backup activity. In case of failures, the SRE team manually triggers the backup script, identifies the root cause & resolves the issue. MoEngage takes AMI images of the servers hosted on AWS. Images for the last seven days are retained. The backups and AMIs are moved to S3 at a different zone within the hosting region. The status of backup is notified to the stakeholders via automated email notification. The backups are monitored manually periodically to ensure their existence and status is updated in the monitoring checklist.

Business Continuity Process

MoEngage takes adequate AMI images and backups of the application & database production instances which can be used for restoration if required. The AMI images of the past seven days are retained.

Data Security & Confidentiality

MoEngage SaaS application is accessed via a web browser over the internet through HTTPS protocol using SSL certificate having SHA-256 with RSA encryption as the Certificate Signature Algorithm. The SSL certificate is generated with 2048 bits. The lock icon in the browser indicates that data is fully encrypted and protected from access while in transit. The certificates are renewed on a yearly basis. The production instance databases are configured on hardened servers. The database resides inside the network segment and has no access to the internet. Sensitive data like keys, tokens, passwords are encrypted while at rest.

Access to data is restricted to authorized applications through access control software. Customer data is not stored in the MoEngage network unless otherwise authorized by the customer. In such scenarios, customer data is stored at a restricted location in customer specific folders. Access to this location is granted only to authorized users after written approval from the manager. All agreements with related parties and vendors include confidentiality commitments consistent with the company's confidentiality policy (as described in Information Security Policy). The local HR and Finance data is stored at a restricted location.

Incident Management Operations

DC4: The Incident identified for the system 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 of those service commitments and system requirements, during the period of 6 months, the following information:

- ***Nature of each incident***
- ***Timing surrounding the incident***
- ***Extent (or effect) of the incident and its disposition***

Incident Reporting and Resolution

Procedures for the incident response including the identification and escalation of customer issues, security breaches, and other incidents are included in the policy. Incidents/complaints are reported to the IT help desk ticketing system. The customers report the issue through the Zendesk ticketing system. When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Based on the severity of the issue, its priority is defined, and a fix is planned accordingly. Critical issues are dealt with topmost priority and provided with a resolution/patch at the earliest. Non-critical issues are fixed as per the devised plan. MoEngage production systems are monitored by the IT team. Any incident (an outage, bug, security vulnerability, etc.) noticed/reported triggers the Incident Response Process.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.

There are no data breach/security incidents during the audit period.

TSC framework & Controls

DC5: The trust services criteria and the related controls designed to provide reasonable assurance that MoEngage service commitments and system requirements were achieved.

Overview of Controls

MoEngage deems internal controls as processes that are developed and implemented by an entity's board of directors, management, and other personnel designed to provide reasonable assurance of achieving the entity's objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of service organization's control reporting.
- Compliance with applicable laws and regulations.

MoEngage further identifies five interrelated components in which to view these categories:

- **Control Environment**–The overarching tone of the organization affects the control consciousness of its people. This is the foundation for all other components of internal control providing discipline and structure.
- **Control Activities**–Policies and procedures that are established and executed to ensure that the actions identified by management as necessary to address risks and achieve the entity's control objectives are effectively carried out.
- **Information and Communication**–Systems, both automated and manual, that are used to identify, capture and exchange information, that allows entity personnel to carry out their responsibilities.
- **Monitoring**–The process of assessing the quality and effectiveness of the internal controls over a period.
- **Risk Management**–The processes used to identify and analyze the risks in achieving its objectives that are the basis for determining how the risks are managed.

Control Philosophy

To assist in MoEngage efforts to protect and secure its information and those of its clients, MoEngage has adopted an Information Security Policy to work in concert with information security and availability methods and procedures. In addition, key operating methods and procedures are documented. This information is presented in this report and further describes MoEngage controls placed in operation.

Control Environment

MoEngage control environment is a collaborative effort of multiple departments to establish and enhance controls and mitigate the risks the business may encounter. It reflects the commitment of management and its company to maintain controls through policies and procedures and organizational structure. MoEngage control environment is examined every six months at a minimum by the internal auditor and annually by independent external auditors.

Integrity and Ethical Values

MoEngage requires officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the company, and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. MoEngage promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Commitment to Competence

MoEngage's formal job descriptions outline the responsibilities and qualifications required for each position in the company. Employees are evaluated on an annual basis to document performance levels against MoEngage values and give feedback in terms of an individual's key strengths and areas of improvements. The employees are also assigned quarterly OKRs to be achieved.

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within MoEngage.

Human Resources Policies and Procedures

MoEngage Human Resources Department follows standard Policies and Procedures for functions like hiring, performance appraisal, termination, and security. Employees are informed of these policies and procedures upon their hiring and sign an acknowledgment form confirming their receipt. Violation from established Human Resources policies and procedures result in disciplinary actions, up to and including employee termination. All relevant policies and procedures are shared over email with all employees.

MoEngage the HR policies includes formal hiring policy. Whenever a new position is to be opened, a Hiring Requisition Form (HRF) is filled and submitted to the HR after seeking approval from the manager. The HRF is also supplemented with detailed Job description stating the qualification, experience, skill-set and roles and responsibilities sought from the candidate. The potential candidates go through a defined interview process which may include but are not limited to the aptitude test, technical test, assignment, audio-video interview, face-to-face discussion depending on the role and team where she/he is being hired.

Control Activities

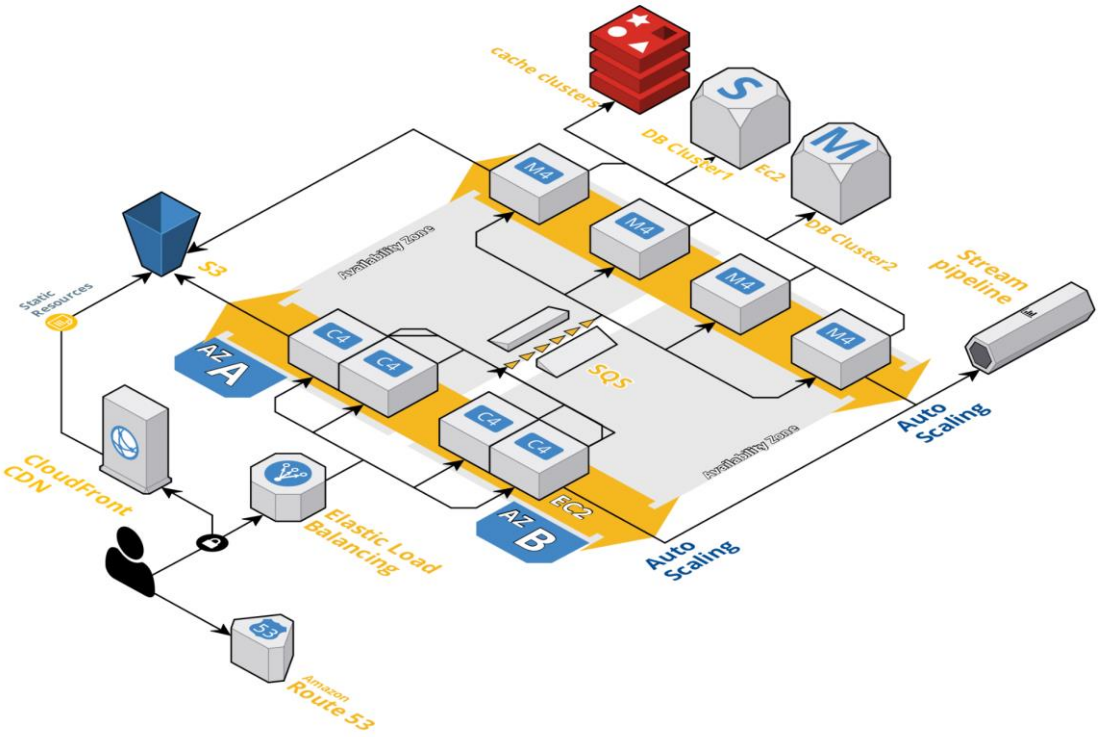
Server Management & Access Policy

MoEngage solution is hosted on Amazon Web Services, in AP-South (Mumbai), US-East (Northern Virginia) and EU-Central (Frankfurt) zone. The servers are solely managed by authorized MoEngage personnel only. MoEngage has defined hardening checklist that is used for configuring the new servers on AWS. The servers are thus hardened and run with minimal services and enhanced security configuration. Unwanted services on application & database servers are turned off.

MoEngage strictly follows restricted & role-based access policy on all servers & only authorized IT personnel are provided access. The access follows the principle of least privilege and is granted only after the written approval from the Manager. Access to the servers follows strong cryptography & uses technologies such as SSH, SSL or VPN to ensure security. VPN access to production instances is restricted to limited support staff of MoEngage. It follows name-based credentials.

Network Security

MoEngage hosts application servers in the DMZ (Demilitarized Zone) segment since they are accessible externally. The DMZ network segment has restricted access to the internet. It's controlled by configuring IP and port-based rules in hardware and software firewall. The database servers are hosted in the Inside Network Segment with no access to the internet. The network is further segregated into Trusted Network and Untrusted Network for enhanced security. MoEngage Web Server routes the incoming requests to the deployed solution. It does not contain any business logic or components. The servers are configured to process only HTTPS requests & other internet protocols are disabled. Refer to the following MoEngage Network Diagram for an overview.



Server Firewall

Communication with servers is routed through a software firewall, Deepfence. It has been configured to allow access to Production servers only from whitelisted IPs. Only the ports that are required for connecting to the external network are opened. Any changes to the firewall are made after formal approval. Firewall events are logged. Access to firewall rules through the web interface is secured. This access is restricted only to authorized Security office personnel. The servers also implement software firewall, IP Tables, to gain fine-grained control over incoming and outgoing traffic.

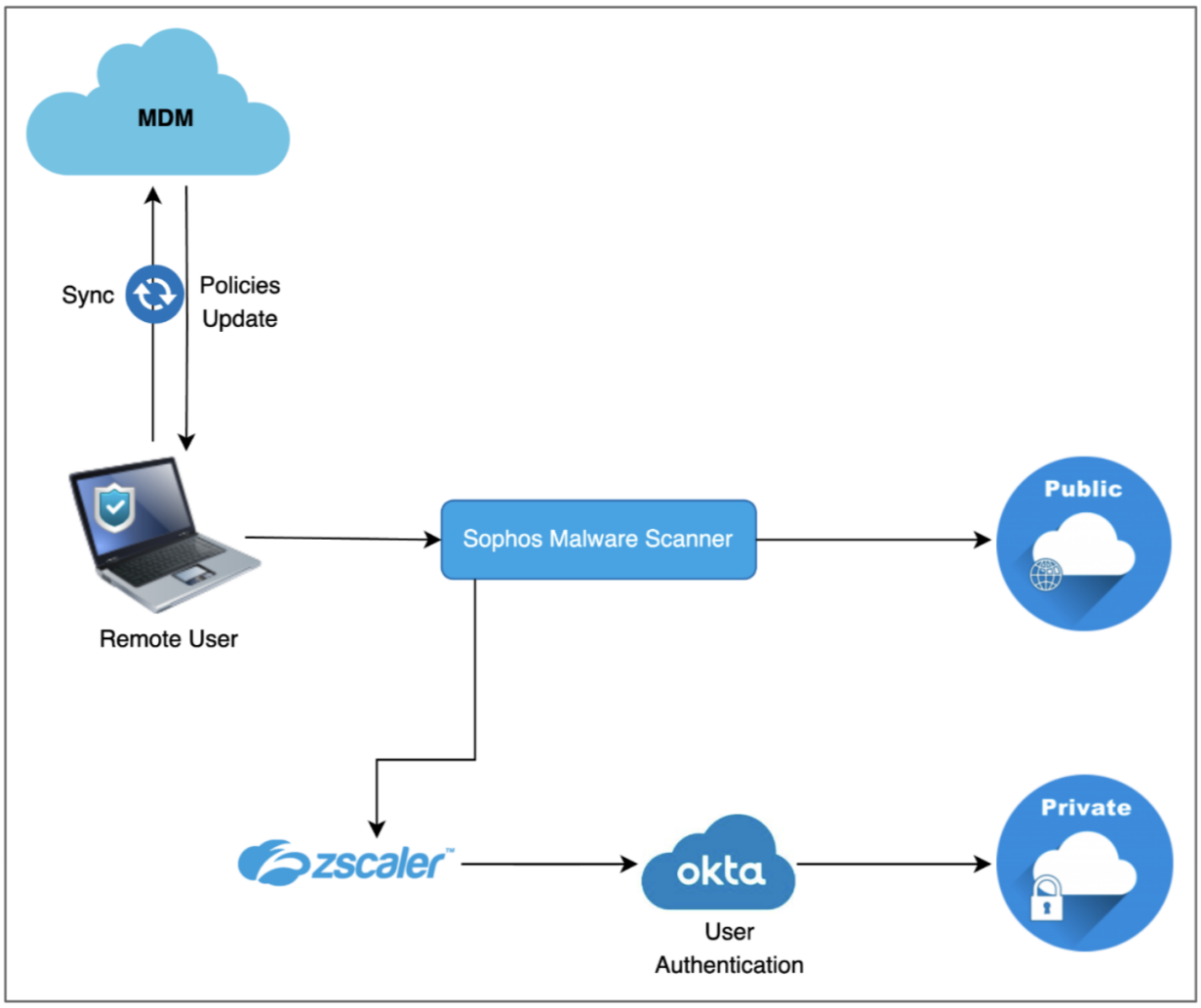
Application Level Security

The customers access MoEngage applications through username and password. The password is stored in encrypted format in the database. The application implements strong security policy which can be customized for every customer as per their requirement. Following security features are supported by our application:

Administrative Level Access

MoEngage is primarily concerned with administrative access to its production infrastructure. Administrative rights and access are restricted to authorized Support personnel. For exceptional cases where admin rights are required by individuals to perform their jobs, it must be justified to and approved by the Head of Security.

Remote/Local Network Architecture



Remote Environment Controls

MoEngage is a cloud first organization, where complete IT Infrastructure is hosted on cloud or utilize SaaS services from other vendors. Complete IT infrastructure is built on a centralized Single Sign-On Server, Okta providing authentication and restricting access to systems within the organization's network.

Host based Security controls are implemented to ensure secure access to scoped applications on a need to know basis. Systems used for projects are configured to be a part of this and are protected by Proxy based Firewall, Anti-virus, MDM, Ransomware protection and DLP solutions.

System logs are maintained. MoEngage VPN gateways are established and managed by the IT Team. The VPN access is granted to a specific IP address after approval from the reporting manager. Authorized employees can then access the production system using VPN only. The VPN authenticates users through name-based access and two factor authentication.

Physical Access & Security

Entry to the MoEngage office is restricted to authorized personnel by card-based access control system and biometrics. All employees are provided with access cards. The cards/biometric authentication open the door lock. Attendance is recorded through biometrics. All visitors must sign the visitors' register and must be escorted in the office.

Employees are required to show their picture ID cards at the Security entrance and finger swipe in the access management system. Employees are granted access only to those areas which they require to access. Access to areas marked as 'Authorized' is tightly controlled on a need basis and needs to be approved by the Head of Security or Sr. Manager Facility. The management team has access to all areas except the 'Authorized' areas like server rooms. Employees are required to wear their access cards/employee identification cards always while within the facility.

Security guards control visitor access at all entrance points. Surveillance cameras have been installed at various critical points within & around the facility. Backup of recordings are stored for a minimum of 90 days.

Logical Access

MoEngage Information Security Policy covers access to computing resources. Default access has been defined for all nonpublic resources. Any additional access needs written approval from designated officers. Access to IT resources follows the principle of least privilege. Users are given name-based access to servers after receiving written approval from the manager. The users are assigned appropriate groups based on their rights. Administrative access is usually restricted to authorized IT personnel only.

When a candidate's joining confirmation is received, HR sends an email to IT helpdesk to set up a new workstation/laptop, which is configured with minimum default access to company resources/applications required by an employee to perform the job duty. Any additional access is recommended by the hiring manager and approved by IT Manager for employees across the regions.

Only the IT team has access to change user profiles or give higher access. Other employees do not have local admin privileges on their laptops. The IT team monitors the installation of software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

Access to the MoEngage network & systems is managed through a Single Sign-On server, Okta Access is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password and two factor authentication. Privileged access to sensitive resources is restricted to defined user roles and access to these roles is approved by senior management.

Access to the Server Room

Access to the server room is controlled by an access control system and granted only to selected IT personnel. Third parties are allowed access to the server room only under the supervision of IT team members.

Firewalls

Network Firewall, restricted access points and device whitelisting is implemented to control external access to the MoEngage network. Firewall events are logged. The firewall has been configured in the India office so that only certain limited services are allowed through the firewalls. Only the ports required for connecting to the external network are opened. This is managed on a host to host basis to safeguard the MoEngage network.

Network & endpoint protection / system monitoring

To stop any malware from affecting the security of the customer and organizational data, MoEngage uses daily Sophos Endpoint Protection scan in the local systems and access point audit on the network. IT team ensures that all the endpoints in organizations are monitored for any vulnerabilities and that any malware is dealt with efficiently and in a timely manner. The company has implemented restrictions such as disabled USB ports, DVD writers, printing, etc. on the workstations through endpoint protected software and device policies. Privileged programs or installing software etc. need admin access which resides only with authorized IT personnel.

Security Authorization and Administration

Access to MoEngage servers is granted through a VPN tunnel only. After the VPN tunnel is established, the servers are accessed via bastion host, StrongDM through single-SignOn server. The users are created with the principle of least privilege. The user is not allowed administrative activities, which are only managed by authorized IT personnel.

MoEngage Information Security Policy covers access to computing resources. Default access has been defined for all nonpublic resources. Any additional access needs approvals from designated officers.

Only the IT team has access to change user profiles or give higher access. Other employees do not have local admin privileges on their laptops. Only the IT team has access to install software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

Access to the MoEngage network & systems is managed through a single sign-on server. Access is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password and two factor authentication. Privileged access to sensitive resources is restricted to defined user roles and access to these roles is approved by senior management.

Access to confidential reports is provided to authorized individuals based on approval. Access to the storage, backup data, systems, and media is limited to the IT team using physical and logical access controls.

Security Configuration

Employees establish their identity to the local network and remote Client systems using a valid unique user ID that is authenticated by an associated password. Password must have the following characteristics.

- Minimum 8 characters
- Complex with at least 1 numeric, 1 special character, 1 Upper Case
- Expires in 90 days
- 5 password history
- Lockout after 5 failed attempts

Passwords are controlled through the Password policy and include periodic forced changes, password expiry, and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT team to reset the password. When IT Team resets the user's password, the user is forced to change the password on the first log on. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Local administrator privilege is restricted to the IT Team and is not available to other users. However, where the project needs the team members to have the local admin access, the respective line manager will raise a request to senior management which can approve or deny the request based on its merit.

Unattended laptops are locked within five minutes of inactivity. Users are required to provide their password to unlock the laptop.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access to perform their jobs. MoEngage is primarily concerned with administrative access to its IT facilities. All administrative level access must be justified to and approved by Head of Security.

Risk Management

Risk Assessment, Monitoring and Mitigation

MoEngage understands its fundamental responsibility to identify, evaluate, and manage business risks related to non-public information and associated processing systems consistent with the best interests of both MoEngage and its customers.

MoEngage has placed into operation a risk assessment process to provide a mechanism for MoEngage management to identify, manage, and report on technology risks to fulfill regulatory responsibilities, as well as improve the efficiency and effectiveness of technology, processes, and services.

This process is followed on a need basis, and it consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

Information Security Team is responsible to monitor organization-level risk and ensure the application of appropriate risk treatment is applied to mitigate the risks and reduce impact on the project execution. high-impact risks are discussed in the management review meetings and approval for any additional resources is obtained as needed.

While the assignment of risk levels is somewhat subjective, the following definitions and criteria provide a guide in assigning risk levels.

MoEngage determines the impact of risk in the below 5 Categories:

- System security [Confidentiality & Integrity]
- Business Interruption [Availability]
- Financial
- Reputation and Image
- People

The Asset Identification and Classification exercise will be carried out that will include gathering data about confidentiality, integrity, and availability (CIA) of information assets.

Asset Criticality Value = C*I*A
Asset Criticality Rating = Asset Criticality Value / 3

Risk impact is rated on a five-point scale from 0 = None to 10 = Critical based on pre-defined criteria in MoEngage Risk Management policy and procedures. Once the Impact of Risk is determined, an estimate of the likelihood of the threat occurring is made.

Risk Likelihood is rated on a 5-point scale of Risk likelihood ranging from 1 = Rare to 5 = Almost Certain.

To assess the risk to determine the appropriate treatment, MoEngage will examine the Risk Level or Inherent Risk, which is the combination of likelihood and impact.

Risk Value/Score = Asset Criticality Rating * Likelihood * Impact.

A combined risk score for likelihood and impact can result in the following Risk Levels:

- Very High [VH] (81-100)
- High [H] (61-80)
- Medium [M] (41-60)
- Low [L] (0-40)

MoEngage evaluates information risk on an ongoing basis as well as when introducing or materially changing facilities, policies, processes, projects, networks, or systems. Such evaluations incorporate the following considerations:

- Business requirements
- Likelihood of loss or compromise if the risk is realized
- The severity of impact if the risk is realized
- Non-public information involved (sensitivity, criticality, volume)
- Associated and connected systems (existing controls, complexity)
- Supporting processes and procedures

MoEngage Information security team compares the results of risk analysis with the risk criteria established above to ensure the risk assessment has adequately covered all criteria.

For those risks that are above the risk acceptable threshold, the options for Risk Treatment will be explored. A risk mitigation strategy will be used in the decision as to which course of action to follow.

The risk treatment plan is used to ensure that potential risks do not become real, or if they do. Contingencies are in place to address them.

The following options may be applied to the treatment and mitigation of identified risks:

- Avoid: Avoid the risk by taking action that means it no longer applies
- Transfer: Transfer the risk to another party e.g., insurer or supplier
- Mitigate: Mitigate the risk by applying appropriate controls to reduce the likelihood and/or impact
- Accept: Accept the risk within the organization

The evaluation of the treatment options will result in the production of the Risk Treatment Plan will detail:

- Risks above the acceptance threshold
- Control requirements or actions to remediate the risk
- Risk owners and approvers

Information Security Policies

MoEngage has developed organization-wide Information Security Policies. Information Security Policies comprising of IT, Facilities, HR and Governance policies & procedures are made available to all employees. Domains within the IT & Security Policies include Access Control, Asset Management, Business Continuity Planning, Change Control, Acceptable Use, and Information Sensitivity.

Changes to the Information Security Policies are reviewed by the InfoSec Team and approved by MoEngage Steering Committee prior to implementation.

Information and Communication

MoEngage has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon changes and approval by management. Departmental managers monitor adherence to the policies and procedures as part of their daily activities.

Electronic Mail (E-mail)

MoEngage uses Google's email service. Customer data is shared over dedicated AWS S3 buckets. Communication with Customer Organizations and project teams happens through E-Mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using E-Mail. E-Mail is also a means to draw the attention of employees towards adherence to specific procedural requirements.

Monitoring

Monitoring & Logging

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. MoEngage management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

The servers and infrastructure are monitored through monitoring tools which monitor vital server parameters, and compliance with infrastructure & network performance commitments. The servers are continuously monitored for vital parameters the server like CPU, Load Average, Disk Usage and Memory utilization. The thresholds are defined for every parameter. If any parameter crosses the defined threshold, automated email notifications are sent to the support team, which takes over the issue thereon. The application uptime is monitored through uptime utility from different geolocation.

System and application logs are consolidated in a centralized log management tool to aid efficient search and event notification.

Complementary User Entity Controls

DC6: MoEngage management assumed, in the design of the MoEngage system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the MoEngage, to provide reasonable assurance that MoEngage's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs).

User- Entity Control Considerations

Services provided by MoEngage to user entities and the controls of MoEngage Systems cover only a portion of the overall controls of each user entity. MoEngage controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve relating to the services outlined in this report to be achieved solely by MoEngage.

This section highlights those internal control responsibilities that MoEngage believes should be present for each user entity and has considered in developing the controls described in the report.

This list does not purport to be and should not be considered a complete listing of the controls relevant at user entities. Other controls may be required at user entities.

- **Contractual Arrangements**
    - User organizations are responsible for understanding and complying with their contractual obligations to MoEngage Systems such as providing input files, review and approval of processed output and releasing any instructions.

- **Other Controls**

    - User Organizations are responsible for ensuring end customer privacy.
    - User Organizations are responsible for ensuring that complete, accurate and timely information is provided to MoEngage for processing.
    - User Organizations are responsible for their network security policy and access management for their networks, application & data.
    - User Organizations are responsible for working with MoEngage to jointly establish service levels and revise the same based on changes in business conditions.
    - User Organization must have Information security policies, procedures, standards, & guidelines
    - Verification & Validation of all data inputs from MoEngage.
    - Verification & Validation of all output reports of MoEngage application.
    - User entity timely deactivation or removal of user accounts for user entity terminated employees previously involved in functions or activities involving systems interfacing with service organization's systems.
    - User organization controls related to system access and acceptable use for all systems that interface with the service organization's systems (directly or indirectly).

Complementary Subservice Organization Control (CSOC)

or Control over Subservice Organization

DC7: If MoEngage uses a sub-service organization and the controls at the sub-service organization are necessary, in combination with controls at MoEngage, to provide reasonable assurance that MoEngage' service commitments and system requirements are achieved, the following:

a. When MoEngage management elects to use the inclusive method:

i. The nature of the service provided by the sub-service organization
ii. The controls at the sub-service organization that are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements are achieved
iii. Relevant aspects of the sub-service organization's infrastructure, software, people, procedures, and data
iv. The portions of the system, that are attributable to the sub-service organization

b. When MoEngage management decides to use the carve-out method:

i. The nature of the service provided by the sub-service organization
ii. Each of the applicable trust services criteria that are intended to be met by controls at the sub-service organization
iii. The types of controls that service organization management assumed, in the design of MoEngage' system, would be implemented by the sub-service organization that are necessary, in combination with controls at MoEngage, to provide reasonable assurance that MoEngage' service commitments and system requirements are achieved (commonly referred to as complementary sub-service organization controls or CSOCs)

MoEngage uses the AWS IaaS platform to offer its SaaS services. MoEngage relies on the SOC reports and ISO/IEC 27001:2013 Certificates of AWS for physical security.

Non-Applicability of any TSC

DC8: MoEngage has claimed non-applicability for --Any specific criterion of the applicable trust services criteria that are not relevant to the system and the reasons it is not relevant.

The TSC Criteria for Processing Integrity and Privacy is marked as non-applicable since the scope of this attestation is limited to Confidentiality, Security and Availability only.

Significant changes to the system framework

and controls during the period under review

DC9: MoEngage changes to system framework and controls
In a description that covers a period of time (type 2 examination), the relevant details of significant changes to MoEngage' system and controls during that period that are relevant to MoEngage' service commitments and system requirements

There are no major changes to any policy, procedure or system framework and controls during the period under review June 1, 2022 to May 31, 2023.

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM v4.0.7)

MoEngage is a Cloud Service Provider (CSP) that provides SaaS services to their customers has defined, documented, implemented, and monitored the following CCM controls.

A&A- Audit and Assurance
AIS- Application & Interface Security
BCR- Business Continuity Mgmt & Op Resilience
CCC- Change Control & Configuration Management
CEK- Cryptography, Encryption and Key Management
DCS- Datacenter Security
DSP- Data Security and Privacy
GRC- Governance, Risk Management and Compliance
HRS- Human Resources Security
IAM- Identity & Access Management
IPY- Interoperability & Portability
IVS- Infrastructure & Virtualization Security
LOG- Logging and Monitoring
SEF- Security Incident Management, E-Discovery & Cloud Forensics
STA- Supply Chain Management, Transparency & Accountability
TVM- Threat & Vulnerability Management
UEM- Universal Endpoint Management

Section-IV

Description & Evaluation of Controls

to achieve the applicable Trust Services Criteria, CCM Criteria and results thereof.

Information provided by the Independent Service Auditor

MoEngage described the system included in Section II and Section III of this report, "Management Assertion" and "Description of Controls provided by MoEngage" respectively. Only the key controls identified by MoEngage Company that support control objectives have been identified in this section.

SOC2 Overview

The AICPA guide 'Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)' guides SOC 2 reports performed under the AICPA attestation requirements and guidance established in SSAE 18, Attest Engagements (AICPA, Professional Standards), Statements on Standards for Attestation Engagements (SSAE). SOC 2 reports replace many reports formerly performed under the SAS 70 (Statement on Auditing Standards No. 70, Service Organizations). SOC 2 provides guidance that allows a service organization such as MoEngage to disclose their control activities and processes and compliance with the applicable Trust Services Criteria to their customers (user organizations) and their customer's knowledgeable interested parties. The criteria for the applicable Trust Services Criteria are based on Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, issued by the AICPA. The service organization employs an independent accounting and auditing firm (service auditor, CPA) to examine their control objectives and control activities. The service auditor issues a Service Auditor's Report to the service organization at the end of the examination that includes the auditor's opinion.

CCM4 Overview

The CCM includes detailed security concepts and principles aligned with CSA Security Guidance v4, which guides "how" security principles should be implemented in a cloud architecture. Conversely, the CCM recommends "what" should be done. The CSA encourages organizations to use the CCM as a companion to the CSA Security Guidance because it allows users to identify security controls and understand how they should be applied. The CCM v4.0 is structured into 17 security domains and 197 controls.

Objectives of the Examination

This report on Controls at a Service Organization relevant to Security, Availability, and Confidentiality, only and the Suitability of the Design of Controls and operating effectiveness is intended to provide interested parties with information enough to understand the basic structure of controls within MoEngage. This report, when coupled with an understanding of controls in place at user locations, is intended to permit evaluation of the total system of internal control surrounding the reviewed systems.

Our examination was restricted to selected services and applicable Trust Services Criteria and CCM Criteria provided to system users by MoEngage and accordingly, did not extend to controls in effect at user locations. It is each interested party's responsibility to evaluate this information concerning controls in place at each user location to assess the total system of internal control. The user and MoEngage portions of the system must be evaluated together. If effective user controls are not in place, MoEngage controls may not compensate for such weakness.

Our examination included interviews with key personnel, a review of available documentation for accessing security and availability criteria as appropriate, and observation and inspection of certain controls surrounding and provided by MoEngage. Our examinations were designed only to clarify the understanding of the information contained in the attached Description. Also, we applied tests to specific controls to obtain evidence about their effectiveness in meeting the related control objectives, pertaining to security and availability criteria.

MoEngage 's relevant control objectives and the relationship of MoEngage's controls to the applicable Trust Services Criteria are presented under the following tables under the heading "Trust Services Criteria Matrices".

Interested parties using this report as part of their review of a user's system of internal controls may conclude that MoEngage's System's Description provides a basis for reliance thereon and for restricting the extent of their substantive tests. Alternatively, interested parties may elect not to rely on controls within MoEngage System's system. In that event, they should accomplish their audit objectives by other means.

The objectives of controls relevant to Trust Services Criteria and CCM Criteria are to provide reasonable, but not absolute, assurance about such things as:

- Security: The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.
- Availability: The system is available for operation and usage to meet the entity's commitments and system requirements.
- Confidentiality: The system information designated as confidential is protected to meet the entity's objectives.
- Processing Integrity and Privacy are out of scope.

The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits derived and, additionally, that evaluation of internal control necessarily requires estimates and judgments by management.

A variety of audit procedures were performed, each of which provided different levels of audit comfort. The combined results of these procedures and tests provided the basis for understanding the framework for control and determining whether the controls represented by MoEngage were operating effectively throughout the period from June 1, 2022 to May 31, 2023.

Criteria, Controls, and Risks

Trust Services Criteria represent attributes of a system (Infrastructure, Software, People, Processes, and Data) that support the achievement of management's objectives.
The 2017 Trust Services Criteria consist of Common Security Criteria (Common Criteria).

- CC1 – Control Environment
- CC2 – Communication and Information
- CC3 - Risk Assessment
- CC4 - Monitoring Activities
- CC5 – Control Activities
- CC6 - Logical and Physical Access Controls
- CC7 - System Operations
- CC8- Change Management
- CC9 - Risk Mitigation
- Additional Principle-specific Criteria.
  A - Additional Criteria for Availability
  C- Additional Criteria for Confidentiality

CCM Criteria

- **A&A-** Audit and Assurance
- **AIS-** Application & Interface Security
- **BCR-** Business Continuity Mgmt & Op Resilience
- **CCC-** Change Control & Configuration Management
- **CEK-** Cryptography, Encryption and Key Management
- **DCS-** Datacenter Security
- **DSP-** Data Security and Privacy
- **GRC-** Governance, Risk Management and Compliance
- **HRS-** Human Resources Security
- **IAM-** Identity & Access Management
- **IPY-** Interoperability & Portability
- **IVS-** Infrastructure & Virtualization Security
- **LOG-** Logging and Monitoring
- **SEF-** Security Incident Management, E-Discovery & Cloud Forensics
- **STA-** Supply Chain Management, Transparency & Accountability
- **TVM-** Threat & Vulnerability Management
- **UEM-** Universal Endpoint Management

The environment in which the system operates, commitments made to customers and other third parties, responsibilities entailed in operating and maintaining a system, and the nature of the components of the system result in risks that the criteria will not be met.

These risks are addressed through the implementation of suitably designed criteria that, if operating effectively, provide reasonable assurance that the criteria are met.

The 'Trust Services Criteria Matrices' herein presents the design and implementation of the system including the specific risks that the criteria will not be met and the controls necessary to address those risks.

Evaluation of Controls

Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing, or maintaining the effectiveness of specific controls. Elements of MoEngage 's control environment include:

- Organizational structure and approach to segregation of duties
- Management control methods
- MoEngage 's policies and practices
- Internal Audit
- Regulation of MoEngage by the regulatory bodies

In developing the tests described in this Section, we evaluated the control environment which included:

- Review of MoEngage 's organizational structure, including the segregation of functional responsibilities, policy statements, processing manuals, policies including internal audit policies, procedures, and reports.
- Discussions with management, operations, administrative, and other employees who are responsible for developing, ensuring adherence to, and applying controls; and
- Observations of employees in the performance of their assigned duties.

Controls

Our tests of the effectiveness of the controls included such tests as we considered necessary in the circumstances to evaluate whether those controls and the extent of compliance with them, was sufficient to provide reasonable but not absolute assurance that the specified control objectives were achieved during the period from June 1, 2022 to May 31, 2023. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions and procedures throughout the period from June 1, 2022 to May 31, 2023, for the controls listed in this section, which are designed by management to achieve the specified control objectives. In selecting a test of the operational effectiveness of controls, the following were considered: the nature of the items being tested,

- The types and competency of available evidential matter,
- The nature of the audit objectives to be achieved,
- The assessed level of control risk and,
- The expected efficiency and effectiveness of the test.

In determining the tests to be conducted, procedures performed by MoEngage's internal audit team were considered. Accordingly, the effectiveness of the internal audit function was evaluated and tested, including.

- an assessment of the independence, competence, and objectivity of the internal audit function,
- an evaluation of the scope of work and the adequacy of audit programs,
- a review of work papers to assess the adequacy of documentation, supervision, and review, and
- an assessment of the conclusions reached, and reports issued.

The types of tests performed concerning the information addressed in this section and of the operating effectiveness of controls as detailed in this section are briefly described below:

Test	**Description**
Inspection	Inspected documents and reports indicating the performance of the control activity.
Re-performance/Transaction	Testing Re-performed application of the control activity.
Observation	Observed application of specific control activities.
Corroborative Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.

The following information pertains to tests of operating effectiveness performed by Independent Auditors. The suitability of design was examined, and the tests were performed only on those controls specifically identified. Testing of the operating effectiveness of identified controls was performed during the period from June 1, 2022 to May 31, 2023. The nature and extent of tests performed, along with the specific control objective they were designed to achieve, are identified for each trust criteria in the table below:

Trust Services Criteria (TSC) 2017

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
Control Environment				
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**			
CC1.1A	Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.	MoEngage's Board of Directors and management demonstrate the importance of integrity and ethical values through a code of conduct documented in the employee handbook.	Inspected Darwinbox screenshots for employees having acknowledged the employee handbook which covers the code of conduct.	No exceptions noted.
CC1.1B	Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	MoEngage has established the code of conduct documented in the employee handbook. At the time of joining MoEngage, every employee is required to read MoEngage corporate policies and procedures and acknowledge them for adherence on the HRMS portal, Darwinbox.	Inspected Darwinbox screenshots for employees having acknowledged the employee handbook which covers the code of conduct.	No exceptions noted.
CC1.1C	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	MoEngage has a process of getting acknowledgment from employees/business partners and conducting employee performance evaluation on a yearly basis.	Inspected sample signed acknowledgment from employees, business partners, outsourced service providers, and sample employee performance evaluation reports with adherence to standards of conduct.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.1D	Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.	MoEngage has defined, documented, reviewed, and implemented disciplinary process for addressing any deviation in timely and consistent manner.	Inspected code of conduct, and HR manual with disciplinary process to address deviations in a timely manner. Inquired the MoEngage management team to understand any deviation cases identified. The management team confirmed that there are no such cases.	No exceptions noted.
CC1.1E	Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	MoEngage has a process of signing agreements with vendor, and business partners.	Inspected sample signed agreements for customers and vendors.	No exceptions noted.
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**			
CC1.2A	Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.	MoEngage has established an organizational structure. The organizational structure of MoEngage provides the overall framework for planning, directing, and controlling operations.	Inspected the organization chart which establishes oversight responsibilities.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.2B	Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.	MoEngage has defined job descriptions with relevant expertise.	Inspected sample job descriptions which provide relevant expertise.	No exceptions noted.
CC1.2C	Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.	MoEngage has a separate Executive Leadership Team (ELT) and management team through an established organizational structure.	Inspected the organization chart.	No exceptions noted.
CC1.2D	Supplements Board Expertise—The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.	MoEngage has InfoSec Steering Committee (ISC) supported by the ELT.	Inspected ISC team roles and responsibilities. ISC team conducts regular meetings to report to management on the security implementation. Inspected the meeting minutes.	No exceptions noted.
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**			
CC1.3A	Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	MoEngage has established an organizational structure. MoEngage considers all structures as part of its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process.	Inspected the organization chart.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.3B	Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	MoEngage has established an organizational structure. MoEngage establishes its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process.	Inspected the organization chart with authorities and responsibilities.	No exceptions noted.
CC1.3C	Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	MoEngage has written job descriptions for each role containing roles/responsibilities and job requirements in terms of skills, qualifications, and experience which are reviewed by management.	Inspected sample job descriptions, roles and responsibilities.	No exceptions noted.
CC1.3D	Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.	MoEngage has written job descriptions for each role containing roles/responsibilities and job requirements in terms of skills, qualifications, and experience are reviewed by management.	Inspected sample job descriptions, roles and responsibilities.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.3E	Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.	MoEngage has agreements with external parties for establishing structures, reporting lines, authorities, and responsibilities.	Inspected sample agreements with external parties.	No exceptions noted.
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**			
CC1.4A	Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.	MoEngage has defined and documented policies and procedures.	Inspected sample policies and procedures.	No exceptions noted.
CC1.4B	Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.	MoEngage has a process of evaluating competence by conducting interviews and identifying training requirement for addressing shortcomings.	Inspected sample performance evaluation reports for sample employees and sample training records.	No exceptions noted.
CC1.4C	Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	MoEngage conducts an induction program covering company profiles, policies, code of conduct, information security processes, and practices.	Inspected employee performance evaluation and sample training records.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.4D	Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.	MoEngage has a planned training program to meet succession requirements.	Inspected sample training records.	No exceptions noted.
CC1.4E	Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	MoEngage has a process of conducting third-party background verification check.	Inspected sample background check reports of sample employees.	No exceptions noted.
CC1.4F	Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	MoEngage has documented the technical competence necessary in job descriptions.	Inspected sample job descriptions that contain technical competency requirements.	No exceptions noted.
CC1.4G	Provides Training to Maintain Technical Competencies— The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	MoEngage has a process of identifying and conducting trainings to maintain technical competencies.	Inspected sample training records.	No exceptions noted.
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.5A	Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.	MoEngage has established an organizational structure providing the authorities and responsibilities.	Inspected the organization chart.	No exceptions noted.
CC1.5B	Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	MoEngage has a performance review and evaluation program conducted every 12 months documented in the employee handbook.	Inspected sample performance review reports.	No exceptions noted.
CC1.5C	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	MoEngage has a performance review and evaluation program conducted every 12 months documented in the employee handbook.	Inspected sample annual performance review reports.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC1.5D	Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	MoEngage conducts cross-skills training for employees to manage excessive pressure.	Inspected sample training records.	No exceptions noted.
CC1.5E	Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.	MoEngage has a process of conducting annual performance evaluation.	Inspected annual employee performance evaluation reports.	No exceptions noted.
Communication and Information				
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**			
CC2.1A	Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.	MoEngage has a process for identifying and prioritizing data and information for internal controls.	Inspected data flow diagram.	No exceptions noted.
CC2.1B	Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.	MoEngage has a process for identifying and prioritizing data and information for internal controls.	Inspected data flow diagram.	No exceptions noted.
CC2.1C	Processes Relevant Data Into Information—Information systems process and transform relevant data into information.	MoEngage has a process of using the collected evidence for analyzing the evidence.	Inspected data flow diagram.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC2.1D	Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	MoEngage has a QA process for maintaining quality throughout processing.	Inspected sample QA review reports.	No exceptions noted.
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**			
CC2.2A	Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	MoEngage has defined and documented communication procedures.	Inspected sample communication mail for internal control.	No exceptions noted.
CC2.2B	Communicates With the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	MoEngage has defined and documented the process for communicating with the board of directors in the communication procedure document.	Inspected sample communication mail with the board of directors.	No exceptions noted.
CC2.2C	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	All employees are encouraged to use and communicate via whistleblower@moengage.com to report anonymous or confidential communication.	Inspected sample communication mail for separate communication.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC2.2D	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.	MoEngage has different methods for communication within and external to the organization.	Inspected sample mail communication.	No exceptions noted.
CC2.2E	Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	MoEngage has a process of communicating responsibilities through mail or alternate channels.	Inspected sample mail communication.	No exceptions noted.
CC2.2F	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.	MoEngage has a separate communication line security@moengage.com to report systems failures, incidents, concerns, and other complaints to personnel.	Inspected sample mail communication.	No exceptions noted.
CC2.2G	Communicates Objectives and Changes to Objectives —The entity communicates its objectives and changes to those objectives to personnel in a timely manner.	MoEngage has a process of communicating objectives and changes to objectives through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC2.2H	Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.	MoEngage has a process of communicating information to improve security knowledge and awareness through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.2I	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.	MoEngage has a process of communicating information about system operations and boundaries through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.2J	Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	MoEngage has a process of communicating information about system objectives through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.2K	Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.	MoEngage has a process of communicating information about system changes through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC2.3A	Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	MoEngage has a process of communicating relevant information to external parties through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.3B	Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.	MoEngage has an open communication channel through the contact us form on the website that enables input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others.	Inspected sample mail communication, contact us form on the website enabling inbound communications.	No exceptions noted.
CC2.3C	Communicates With the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.	MoEngage has a process of communicating all assessment results to the board of directors through mails or meetings.	Inspected sample mail communication.	No exceptions noted.
CC2.3D	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	MoEngage has a separate communication line to enable whistle-blower, anonymous or confidential communication when normal channels are ineffective.	Inspected sample mail communication.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC2.3E	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	MoEngage has defined and documented a communication policy for relevant method of communication.	Inspected sample communication through mail, and Slack.	No exceptions noted.
CC2.3F	Communicates Objectives Related to Confidentiality and Changes to Objectives— The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.	MoEngage has a process of communicating objectives related to confidentiality and changes to objectives through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.3G	Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
CC2.3H	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.	MoEngage has a process of communicating information about system operations and boundaries through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC2.3I	Communicates System Objectives—The entity communicates its system objectives to appropriate external users.	MoEngage has a process of communicating information about system objectives through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.3J	Communicates System Responsibilities—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.	MoEngage has a process of communicating information about system responsibilities through mail or alternate communication channels.	Inspected sample mail communication.	No exceptions noted.
CC2.3K	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	MoEngage has a separate communication line security@moengage.com to report systems failures, incidents, concerns, and other matters to personnel.	Inspected sample mail communication.	No exceptions noted.
Risk Assessment				
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**			
	Operations Objectives			
CC3.1A	Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.1B	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.1C	Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.1D	Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
	External Financial Reporting Objectives			
CC3.1E	Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.	As the evaluation of financial controls is out of the scope of this engagement, this control is not applicable.	NA.	NA.
CC3.1F	Considers Materiality—Management considers materiality in financial statement presentation.	As the evaluation of financial controls is out of the scope of this engagement, this control is not applicable.	NA.	NA.
CC3.1G	Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.	As the evaluation of financial controls is out of the scope of this engagement, this control is not applicable.	NA.	NA.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
	External Nonfinancial Reporting Objectives			
CC3.1H	Complies With Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.	MoEngage has defined and documented risk management policy, procedure, and risk register which complies with the ISO framework.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.1I	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.1J	Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
	Internal Reporting Objectives			
CC3.1K	Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.1L	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.1M	Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
	Compliance Objectives			
CC3.1N	Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	MoEngage documented the applicable list of external laws and regulations.	Inspected applicable list of external laws and regulations.	No exceptions noted.
CC3.1O	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.1P	Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**			
CC3.2A	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.2B	Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.2C	Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.2D	Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.2E	Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.2F	Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.2G	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties—The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.2H	Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**			
CC3.3A	Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.3B	Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.3C	Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.3D	Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.3E	Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**			
CC3.4A	Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.4B	Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC3.4C	Assesses Changes in Leadership—The entity considers changes in management and respective attitudes and philosophies on the system of internal control.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.4D	Assess Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC3.4E	Assess Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
Monitoring Activities				
CC4.1	**COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**			
CC4.1A	Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.	MoEngage conducts internal and external audits for ongoing and separate evaluations.	Inspected internal audit reports for ongoing and separate evaluations.	No exceptions noted.
CC4.1B	Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.	MoEngage conducts analysis on audit reports.	Inspected internal audit report and management review meeting minutes for considering the rate of changes.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC4.1C	Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	MoEngage maintains version history in all policies, procedures, guidelines, network diagram, and system hardening.	Inspected version history in all policies, procedures, and network diagram.	No exceptions noted.
CC4.1D	Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	MoEngage has competent people to perform ongoing audits.	Inspected sample job descriptions.	No exceptions noted.
CC4.1E	Integrates With Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.	MoEngage has risk management conducted at various levels.	Inspected internal and external audit reports.	No exceptions noted.
CC4.1F	Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.	MoEngage conducts risk-based audits.	Inspected internal audit report.	No exceptions noted.
CC4.1G	Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.	MoEngage has metrics and measurements process.	Inspected metrics and measurements.	No exceptions noted.
CC4.1H	Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.	MoEngage has a process of conducting independent ISO certification audits and SOC audits annually.	Inspected annual ISO certification and SOC audit report.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC4.2	**COSO Principle 17: 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.**			
CC4.2A	Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.	MoEngage has a process of collecting and analyzing metrics and measurements annually.	Inspected annual metrics and measurements report.	MoEngage needs to be more proactive in assessing metrics and measurements related to ISMS.
CC4.2B	Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	MoEngage has a process of communicating deficiencies to the management.	Inspected sample communication mails related to deficiencies sent to management.	No exceptions noted.
CC4.2C	Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	MoEngage has a process of conducting root cause analysis and corrective actions on all deficiencies annually.	Inspected annual audit report.	MoEngage needs to be more proactive in monitoring RCA, correction, and corrective action tracker, corrective action reports for the nonconformities identified.
Control Activities				
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**			
CC5.1A	Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC5.1B	Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC5.1C	Determines Relevant Business Processes—Management determines which relevant business processes require control activities.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC5.1D	Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC5.1E	Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC5.1F	Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.	MoEngage has defined roles and responsibilities, job descriptions for assigning, limiting authorities, responsibilities, and segregation of duties through change management.	Inspected sample change management tickets which addresses segregation of duties.	No exceptions noted.
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**			
CC5.2A	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC5.2B	Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC5.2C	Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	MoEngage has defined and documented relevant security management process related to risk management, encryption enablement, and role-based access review.	Inspected risk management policy, procedure, and risk register.	No exceptions noted.
CC5.2D	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	MoEngage has defined and documented risk and change management policy, procedures, risk register, and change logs.	Inspected risk management policy, procedure, and risk register and change logs.	No exceptions noted.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC5.3A	Establishes Policies and Procedures to Support Deployment of Management 's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	MoEngage has defined and documented policies and procedures related to security, availability and confidentiality, job descriptions, and segregation of duties.	Inspected policies and procedures which provide management directives.	No exceptions noted.
CC5.3B	Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.	MoEngage establishes responsibility and accountability through roles and responsibilities, job description, and organization structure.	Inspected organization chart and sample job descriptions.	No exceptions noted.
CC5.3C	Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.	MoEngage performs annual audits, and management review meeting as defined in the policies and procedures.	Inspected annual audit reports and management review meeting minutes.	No exceptions noted.
CC5.3D	Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.	MoEngage has a process of conducting root cause analysis and corrective actions by responsible personnel annually.	Inspected annual audit report and NC log with list of findings, RCA, corrections, and corrective actions by responsible personnel.	No exceptions noted.
CC5.3E	Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.	MoEngage has competent people to perform control activities.	Inspected audit reports prepared by competent personnel.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC5.3F	Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	MoEngage conducts an annual review of policies and procedures.	Inspected version history in policies and procedures.	No exceptions noted.
Logical and Physical Access Controls				
CC6.1	**The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**			
CC6.1A	Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.	MoEngage has a process of identifying and managing the inventory of information assets, information processing, and critical assets.	Inspected sample asset inventory list which contains the information of inventory of information assets, information processing, and critical assets.	No exceptions noted.
CC6.1B	Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	MoEngage has a process of restricting logical access by access control policy with the least privilege.	Inspected access management policy and user access list for restricting logical access.	No exceptions noted.
CC6.1C	Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.	MoEngage provides a unique id to identify and authenticate all users.	Inspected access management policy, user access list and Okta screenshots for MFA enablement.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.1D	Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	MoEngage has defined and documented the SaaS infrastructure diagram with relevant segmentation.	Inspected the SaaS infrastructure diagram.	No exceptions noted.
CC6.1E	Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.	MoEngage shows the points of access in the network diagram.	Inspected network diagram showing the point of access.	No exceptions noted.
CC6.1F	Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.	MoEngage provides a unique id to identify and authenticate all their users/employees for restricting unauthorized access to information assets.	Inspected access management policy and user access list showing information assets access.	No exceptions noted.
CC6.1G	Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software.	MoEngage has defined, documented, and implemented a role-based access mechanism for managing the identification and authentication of users.	Inspected role-based access list screenshot which manages identification and authentication.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.1H	Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	MoEngage has defined, documented, and implemented managing credentials for infrastructure and software when no longer required.	Inspected access management policy and user access list which manages credentials for infrastructure and software.	No exceptions noted.
CC6.1I	Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.	MoEngage has defined, documented, and implemented an encryption process to protect the data at rest.	Inspected encryption enablement screenshots that use encryption to protect data.	No exceptions noted.
CC6.1J	Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.	MoEngage has a process of protecting and managing the encryption keys.	Inspected encryption key management screenshots using AWS KMS.	No exceptions noted.
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.**			
CC6.2A	Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.	MoEngage has defined, documented, and implemented access control management for logical access.	Inspected access management policy and user access list for protected assets.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.2B	Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.	MoEngage has a process of revoking user and system access when no longer required.	Inspected access management policy and revoked user access list.	No exceptions noted.
CC6.2C	Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.	MoEngage has a process of reviewing the access for the users and systems.	Inspected access management policy and user access review reports.	No exceptions noted.
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.**			
CC6.3A	Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	MoEngage has defined, documented, and implemented access control management for logical access to protected information assets.	Inspected access management policy and privileged user access list.	No exceptions noted.
CC6.3B	Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.	MoEngage has a process of revoking user and system access for protected information assets when no longer required.	Inspected access management policy and revoked privileged user access list.	No exceptions noted.
CC6.3C	Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.	MoEngage has a process of providing role-based access to support the segregation of incompatible functions.	Inspected role-based user access list.	No exceptions noted.
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.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.4A	Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.	MoEngage has defined, documented, and implemented access control management related to physical access for protecting data centers, office spaces, and work areas.	Inspected physical access control list.	No exceptions noted.
CC6.4B	Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.	MoEngage has a process of revoking physical access when no longer required.	Inspected physical access control list.	No exceptions noted.
CC6.4C	Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	MoEngage has a process of reviewing the physical access control list for protecting data centers, office spaces, and work areas.	Inspected physical access review report.	No exceptions noted.
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.**			
CC6.5A	Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	MoEngage has defined, documented, and implemented a disposal process for identifying data and software for disposal.	Inspected evidence of data disposal for data and software.	No exceptions noted.
CC6.5B	Removes Data and Software From Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.	MoEngage has a process of removing and destroying the data and software from entity control.	Inspected evidence of data and software removal from entity control.	No exceptions noted.
CC6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.6A	Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	MoEngage has a process of restricting access to the FTP site, and router port through firewall rules.	Inspected firewall rules for restricting access to the FTP site, and router port.	No exceptions noted.
CC6.6B	Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.	MoEngage has a process of TLS and SSL for protecting Identification and authentication credentials during data in transit.	Inspected TLS/SSL enablement screenshots for protecting identification and authentication credentials.	No exceptions noted.
CC6.6C	Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.	MoEngage has a process of enabling MFA for additional authentication requirements.	Inspected Okta screenshot showing MFA enablement.	No exceptions noted.
CC6.6D	Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	MoEngage has a process of setting up firewall rules, IDS, and IPS for implementing boundary protection.	Inspected VPC implementation for boundary protection systems.	No exceptions noted.
CC6.7	**The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**			
CC6.7A	Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information.	MoEngage has defined, documented, and implemented data loss prevention.	Inspected DLP configuration screenshots for restricting the ability to transfer data outside the MoEngage environment.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.7B	Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	MoEngage has a process of TLS and SSL for protecting Identification and authentication credentials during data in transit.	Inspected TLS/SSL enablement screenshots by using encryption technologies and secured communication channels.	No exceptions noted.
CC6.7C	Protects Removal Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and back-up tapes), as appropriate.	MoEngage has a process of disabling removal media.	Inspected sample screenshots of tool configuration for disabling removal media.	No exceptions noted.
CC6.7D	Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones and tablets) that serve as information assets.	MoEngage has defined, documented, and implemented a process for protecting mobile devices.	Inspected sample screenshots of tool configuration for protecting mobile devices.	No exceptions noted.
CC6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**			
CC6.8A	Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals.	MoEngage has a process of restricting users from installing applications and software.	Inspected privileged user access list for applications and software installation.	No exceptions noted.
CC6.8B	Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.	MoEngage has a process of detecting changes to software and configuration parameters.	Inspected monitoring logs for software and configuration parameters.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC6.8C	Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change tickets which defines the change control process.	No exceptions noted.
CC6.8D	Uses Antivirus and Anti-Malware Software—Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.	MoEngage has defined and documented policies and procedures on virus controls and threats from malicious software using Sophos antivirus.	Inspected antivirus policy and Sophos configurations and dashboard screenshots.	No exceptions noted.
CC6.8E	Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.	MoEngage has defined and documented policies and procedures on virus controls and threats from malicious software using Sophos antivirus.	Inspected antivirus policy and Sophos configurations and dashboard screenshots.	No exceptions noted.
System Operations				
CC7.1	**To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**			
CC7.1A	Uses Defined Configuration Standards—Management has defined configuration standards.	MoEngage has defined, documented, and implemented configuration standards.	Inspected configuration management policy and list of configurable items.	No exceptions noted.
CC7.1B	Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	MoEngage has a process of monitoring infrastructure and software.	Inspected sample infrastructure and software monitoring alerts and dashboard screenshots.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.1C	Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	MoEngage has a process for creating alerts for changes in file integrity, critical system files, configuration files, or content files.	Inspected file integrity monitoring software and sample change tickets for implementing change detection mechanisms.	No exceptions noted.
CC7.1D	Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.	MoEngage has a process for creating alerts for unauthorized components or access.	Inspected sample monitoring logs screenshots for detecting unknown or unauthorized components.	No exceptions noted.
CC7.1E	Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	MoEngage has a process of conducting third-party VAPT.	Inspected internal and external VAPT reports.	No exceptions noted.
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.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.2A	Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	MoEngage has implemented a CloudTrail tool for detecting anomalies in the operation or unusual activity on systems.	Inspected sample CloudTrail monitoring log screenshots.	No exceptions noted.
CC7.2B	Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	MoEngage has a process for detecting anomalies in the operation or unusual activity on systems.	Inspected sample Deepfence and Kavach tools monitoring screenshots.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.2C	Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	MoEngage has a process of analyzing anomalies to identify security events.	Inspected sample Deepfence and Kavach tools monitoring screenshots.	No exceptions noted.
CC7.2D	Monitors Detection Tools for Effective Operation—Management has implemented processes to monitor the effectiveness of detection tools.	MoEngage has a process of monitoring tools for effective operation.	Inspected sample Deepfence and Kavach tools monitoring screenshots.	No exceptions noted.
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.**			
CC7.3A	Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.	MoEngage has defined, documented, and implemented security IT Security Incident Response Plan and Information Security Policy covering incident response.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.
CC7.3B	Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	MoEngage has a process of communicating and reviewing security events with corrective actions.	Inspected sample communication mails on security events.	No exceptions noted.
CC7.3C	Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.	MoEngage has a process for analyzing security incidents.	Inspected sample incident report covering root cause analysis, correction, corrective action taken, and lessons learned.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.3D	Assesses the Impact on Personal Information—Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
CC7.3E	Determines Personal Information Used or Disclosed—When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
CC7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**			
CC7.4A	Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.	MoEngage has defined, documented, and implemented IT Security Incident Response Plan and Information Security Policy documents with roles and responsibilities.	Inspected IT Security Incident Response Plan and Information Security Policy which contains roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program, and sample incident report.	No exceptions noted.
CC7.4B	Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.	MoEngage has defined, documented, and implemented IT Security Incident Response Plan and Information Security Policy documents for containing security incidents.	Inspected IT Security Incident Response Plan and Information Security Policy which provides details for containing security incidents, and sample incident report.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.4C	Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.	MoEngage has defined, documented, and implemented IT Security Incident Response Plan and Information Security Policy documents for mitigating the effects of security incidents.	Inspected IT Security Incident Response Plan and Information Security Policy, and sample incident report which provides details for mitigating the ongoing security incidents.	No exceptions noted.
CC7.4D	Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	MoEngage has a process of ending threats posed by security incidents.	Inspected IT Security Incident Response Plan and Information Security Policy, and sample incident report which ends the threats posed by security incidents.	No exceptions noted.
CC7.4E	Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.	MoEngage has a process of restoring data and business operations to an interim state.	Inspected backup restoration test and business operations screenshots to an interim state.	No exceptions noted.
CC7.4F	Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	MoEngage has a process of developing, implementing, and communicating security incidents to relevant stakeholders through the mail.	Inspected sample communications related to security incidents with relevant stakeholders on action taken for security incidents.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.4G	Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	MoEngage has defined, documented, and implemented IT Security Incident Response Plan and Information Security Policy documents for containing security incidents.	Inspected IT Security Incident Response Plan and Information Security Policy which provides containment strategy for security incidents and sample incident report.	No exceptions noted.
CC7.4H	Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.	MoEngage has a process of conducting VAPT after remediating all identified vulnerabilities.	Inspected remediated VAPT report to ensure all identified vulnerabilities are remediated.	No exceptions noted.
CC7.4I	Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.	MoEngage has a process of communicating remediation activities to the relevant stakeholder in accordance with the incident response program.	Inspected sample communication mail for communicating remediation activities to the relevant stakeholders.	No exceptions noted.
CC7.4J	Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.	MoEngage has a process of evaluating the effectiveness of the incident response.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report to evaluate the effectiveness of incident response on an annual basis.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.4K	Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.	MoEngage has a process of evaluating the effectiveness of security incidents in the management review meeting on an annual basis.	Inspected management review meeting minutes with incident information.	No exceptions noted.
CC7.4L	Communicates Unauthorized Use and Disclosure—Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
CC7.4M	Application of Sanctions—The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
CC7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**			
CC7.5A	Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	MoEngage has a process of restoring the affected environment with the backup of the system, software, and infrastructure.	Inspected backup restoration test reports.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.5B	Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).	MoEngage has a process of communicating event information with the management and relevant stakeholders.	Inspected sample communication mail about the security event.	No exceptions noted.
CC7.5C	Determines Root Cause of the Event—The root cause of the event is determined.	MoEngage has a process of determining root cause analysis and action taken of the event.	Inspected incident management policy, procedure, and sample incident report with root cause analysis for security events.	No exceptions noted.
CC7.5D	Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.	MoEngage has a process of implementing changes to prevent and detect recurrences of security events.	Inspected sample change tickets.	No exceptions noted.
CC7.5E	Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.	MoEngage has a process of documenting lessons learned and identifying improvements in the incident response and recovery procedures.	Inspected incident management policy and sample incident report with lessons learned for incident response and recovery procedures improvement.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC7.5F	Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	MoEngage has a process of implementing incident recovery plan testing.	Inspected evidence of BC/DR updated and tested plan for incident recovery plan testing.	No exceptions noted.
Change Management				
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.**			
CC8.1A	Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software and procedures) is used to support system availability and processing integrity.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1B	Authorizes Changes—A process is in place to authorize system changes prior to development.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1C	Designs and Develops Changes—A process is in place to design and develop system changes.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change management tickets.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC8.1D	Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1E	Tracks System Changes—A process is in place to track system changes prior to implementation.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1F	Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.	MoEngage has defined, documented, and implemented a change management process.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1G	Tests System Changes—A process is in place to test system changes prior to implementation.	MoEngage has a process of testing the system changes prior to implementation.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1H	Approves System Changes—A process is in place to approve system changes prior to implementation.	MoEngage has a process of approving the system changes prior to implementation.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1I	Deploys System Changes—A process is in place to implement system changes.	MoEngage has a process of deploying the system changes prior to implementation.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1J	Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.	MoEngage has a process of identifying and evaluating the system changes throughout the system development lifecycle.	Inspected change management policy and sample change management tickets.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC8.1K	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.	MoEngage has a process of identifying changes in infrastructure, data, software, and procedures required to remediate incidents.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1L	Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.	MoEngage has a process of maintaining baseline configuration of IT and control systems.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1M	Provides for Changes Necessary in Emergency Situations —A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).	MoEngage has a process for addressing emergency changes.	Inspected change management policy and sample change management tickets.	No exceptions noted.
CC8.1N	Protects Confidential Information—The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.	MoEngage has a process of protecting confidential information by classification of information, access control with MFA enablement, data encryption at data at rest and transit, and signing an NDA.	Inspected MFA enablement screenshots, encryption enablement screenshots, and signed NDA.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC8.1O	Protects Personal Information—The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
Risk Mitigation				
CC9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**			
CC9.1A	Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts.	MoEngage has defined and documented the risk management process in risk assessment policy and procedure.	Inspected risk assessment policy, procedure, and risk register.	No exceptions noted.
CC9.1B	Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	MoEngage has liability insurance to mitigate financial impact risks.	Inspected liability insurance document for mitigating financial impact risks.	No exceptions noted.
CC9.2	**The entity assesses and manages risks associated with vendors and business partners.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC9.2A	Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	MoEngage has agreements with external parties for the scope of services and product specifications, roles and responsibilities, compliance requirements, and service levels.	Inspected sample agreements with external parties which establishes requirements for vendor and business partner engagements.	No exceptions noted.
CC9.2B	Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.	MoEngage has defined and documented risk assessment policy, procedure, and risk register for vendors and business partners.	Inspected supplier management policy and risk register which assess risks related to vendor and business partners.	No exceptions noted.
CC9.2C	Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.	MoEngage has defined and documented risk management policy, procedure, and risk register for vendors and business partners.	Inspected roles and responsibilities documented for managing risks related to vendors and business partners.	No exceptions noted.
CC9.2D	Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	MoEngage has a process of communicating through mail or alternate communication channels with vendors and business partners.	Inspected sample communication mail with vendors and business partners.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC9.2E	Establishes Exception Handling Procedures From Vendors and Business Partners —The entity establishes exception handling procedures for service or product issues related to vendors and business partners.	MoEngage has a process of evaluating SLA and coming out with corrective action for exception handling with reference to service and product issues.	Inspected sample vendor security review report.	No exceptions noted.
CC9.2F	Assesses Vendor and Business Partner Performance—The entity periodically assesses the performance of vendors and business partners.	MoEngage has a process of conducting performance evaluation through vendor audits or vendor performance evaluation checklist.	Inspected sample vendor security review report.	No exceptions noted.
CC9.2G	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.	MoEngage has a process of evaluating issues identified during vendor and business partner assessments.	Inspected sample vendor security review report.	No exceptions noted.
CC9.2H	Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.	MoEngage has a process of terminating the vendor.	Inspected the procedure documented for terminating vendor and business partner relationships.	No exceptions noted.
CC9.2I	Obtains Confidentiality Commitments from Vendors and Business Partners—The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.	MoEngage has a process of signing NDA with vendors and business partners.	Inspected signed NDA with vendors and business partners.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
CC9.2J	Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.	MoEngage has a process of signing an NDA with vendors and business partners.	Inspected signed NDA with vendors and business partners.	No exceptions noted.
CC9.2K	Obtains Privacy Commitments from Vendors and Business Partners—The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
CC9.2L	Assesses Compliance with Privacy Commitments of Vendors and Business Partners— On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.	As privacy criteria is out of scope for this engagement, this control is not applicable.	NA.	NA.
Additional Criteria for Availability				
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.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
A1.1A	Measures Current Usage—The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.	MoEngage has a process of measuring the current usage in the form of a capacity management report with target and current usage and taking corrective action in case of any deviation.	Inspected sample capacity monitoring reports and corrective actions.	No exceptions noted.
A1.1B	Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.	MoEngage has a process of forecasting capacity for various system components.	Inspected sample capacity monitoring reports, and autoscaling feature enabled screenshots.	No exceptions noted.
A1.1C	Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.	MoEngage has implemented an autoscaling feature.	Inspected sample capacity monitoring reports, and autoscaling feature enabled screenshots.	No exceptions noted.
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.**			
A1.2A	Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.	MoEngage is implemented on the AWS data centers and hence relies on AWS for environmental and other relevant controls.	NA.	NA.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
A1.2B	Designs Detection Measures—Detection measures are implemented to identify anomalies that could result from environmental threat events.	MoEngage is implemented on the AWS data centers and hence relies on AWS for environmental and other relevant controls.	NA.	NA.
A1.2C	Implements and Maintains Environmental Protection Mechanisms— Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events.	MoEngage is implemented on the AWS data centers and hence relies on AWS for environmental and other relevant controls.	NA.	NA.
A1.2D	Implements Alerts to Analyze Anomalies—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.	MoEngage is implemented on the AWS data centers and hence relies on AWS for environmental and other relevant controls.	NA.	NA.
A1.2E	Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem).	MoEngage is implemented on the AWS data centers and hence relies on AWS for environmental and other relevant controls.	NA.	NA.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
A1.2F	Communicates and Reviews Detected Environmental Threat Events—Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.	MoEngage is implemented on the AWS data centers and hence relies on AWS for environmental and other relevant controls.	NA.	NA.
A1.2G	Determines Data Requiring Backup—Data is evaluated to determine whether backup is required.	MoEngage has a process of identifying data to be backed up as and when required.	Inspected sample backup logs.	No exceptions noted.
A1.2H	Performs Data Backup—Procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur.	MoEngage has defined, documented, reviewed, and implemented a data backup policy.	Inspected sample backup logs.	No exceptions noted.
A1.2I	Addresses Offsite Storage—Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.	As MoEngage uses a cloud environment, offsite storage is not applicable.	NA.	NA.
A1.2J	Implements Alternate Processing Infrastructure—Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	MoEngage has configured alternate available zones for processing with relevant infrastructure.	Inspected the procedure for implementing alternate processing infrastructure with relevant evidence of alternate zone configuration.	No exceptions noted.
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**			

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
A1.3A	Implements Business Continuity Plan Testing—Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	MoEngage has defined, documented, reviewed, and implemented BCP testing as part of the business continuity plan/disaster recovery plan.	Inspected business continuity and disaster recovery policy, and procedure and updated BC/DR plan and test reports.	No exceptions noted.
A1.3B	Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.	MoEngage has defined, documented, reviewed, and implemented backup and restoration testing as part of the business continuity plan/disaster recovery plan.	Inspected business continuity and disaster recovery policy, and procedure and updated BC/DR plan and test reports.	No exceptions noted.
Additional Criteria for Confidentiality				
C1.1	**The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**			
C1.1A	Identifies Confidential information—Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	MoEngage has defined, documented, reviewed, and implemented a data classification policy to identify confidential information.	Inspected data classification policy, identified confidential information and sample signed NDA.	No exceptions noted.

TSC #	Common Criteria	Description & Design of Controls	Evaluation of Controls	Remarks
C1.1B	Protects Confidential Information from Destruction—Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.	MoEngage has defined, documented, reviewed, and implemented encryption for data, data in transit, and access control policy with MFA, the process of signing agreements, and NDA with employees and third parties.	Inspected MFA enablement screenshots, encryption enablement screenshots, and sample signed NDA.	No exceptions noted.
C1.2	**The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**			
C1.2A	Identifies Confidential Information for Destruction—Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	MoEngage has defined, documented, reviewed, and implemented a secure disposal process, and data retention process.	Inspected sample records of secure disposal and sample signed NDA.	No exceptions noted.
C1.2B	Destroys Confidential Information—Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	MoEngage has defined, documented, reviewed, and implemented a secure disposal process for destroying confidential information.	Inspected sample records of secure disposal and sample signed NDA.	No exceptions noted.

Cloud Control Matrix 4.0.7

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
Audit & Assurance - A & A				
A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	MoEngage has defined and documented audit and assurance policies with version controls and reviews them on an annual basis.	Inspected audit reports.	No exceptions noted.
A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	MoEngage conducts internal and external audits bi-annually and annually.	Inspected audit reports.	No exceptions noted.
A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	MoEngage conducts internal and external audits bi-annually and annually.	Inspected audit reports.	No exceptions noted.
A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	MoEngage conducts internal and external audits bi-annually and annually.	Inspected audit reports.	No exceptions noted.
A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	MoEngage has defined and documented audit and assurance policies with version controls and reviews them on an annual basis.	Inspected internal audit report and management review procedure, ISMS corrective and preventive action procedure.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	MoEngage has defined and documented audit and assurance policies with version controls and reviews them on an annual basis.	Inspected internal audit report.	MoEngage needs to be more proactive in monitoring RCA, correction, and corrective action tracker, corrective action reports for the nonconformities identified.
Application & Interface Security- AIS				
AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	MoEngage has defined and documented Secured Development Guidelines with version controls and reviews them on an annual basis.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports.	No exceptions noted.
AIS-02	Establish, document and maintain baseline requirements for securing different applications.	MoEngage has defined and documented Secured Development Guidelines with version controls and reviews them on an annual basis.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports.	No exceptions noted.
AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	MoEngage has defined and documented Secured Development Guidelines with version controls and reviews them on an annual basis.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports. Inspected metrics dashboard from BurpSuite.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	MoEngage has defined and documented Secured Development Guidelines with version controls and reviews them on an annual basis.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports.	No exceptions noted.
AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	MoEngage conducts Web application Penetration test and external penetration test.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports.	No exceptions noted.
AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	MoEngage has defined and documented Secured Development Guidelines with version controls and reviews them on an annual basis.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports.	No exceptions noted.
AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	MoEngage has defined and documented Secured Development Guidelines with version controls and reviews them on an annual basis.	Inspected secured development lifecycle review checklist for design and testing. Inspected VAPT reports.	No exceptions noted.
Business Continuity Management & Operational Resilience				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test reports.	No exceptions noted.
BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Impact Assessment carried out for people, services and processes as part of business continuity plan implementation.	No exceptions noted.
BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test reports, BIA report Test Plan, and Test reports.	No exceptions noted.
BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test reports, BIA report, Test Plan, and Test reports.	No exceptions noted.
BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test reports, BIA report, Test Plan, and Test reports.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test screenshot, BCP DR test plan, and test report.	No exceptions noted.
BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected sample communication mails.	No exceptions noted.
BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Backup restoration test screenshot.	No exceptions noted.
BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test screenshot, BCP DR test plan, and test report.	No exceptions noted.
BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	MoEngage has defined and documented the Business Continuity plan and Backup restoration test procedure document with version controls and review details.	Inspected Business Continuity plan and Backup restoration test screenshot, BCP DR test plan, and test report.	No exceptions noted.
BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	MoEngage does not rely on any one specific data center for its continued operation and allocates redundant equipment, applications, services and data across multiple data centers.	Inspected Business Continuity plan and Backup restoration test screenshot, BCP DR test plan, and test report.	No exceptions noted.
Change Control & Configuration Management- CCC				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	MoEngage has defined and documented the risk management process integrated with the change management process within the organization.	Inspected Risk Register, Jira tool report and sample change tickets.	No exceptions noted.
CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	MoEngage maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle).	Inspected Jira tool report and sample change tickets.	No exceptions noted.
CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	MoEngage has defined and documented the risk management process integrated with the change management process within the organization.	Inspected Risk Register and Jira tool report.	No exceptions noted.
CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	MoEngage has change management policies and procedures in place to restrict unauthorized changes to MoEngage applications, services, and systems.	Inspected Jira tool report and sample change tickets.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	MoEngage provides customers an advance notice for all system changes having an impact on their environment.	Inspected status.moengage.com site for tracking Client SLA.	No exceptions noted.
CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	MoEngage develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Inspected Jira tool report, and GitHub Audit log.	No exceptions noted.
CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	MoEngage maintains configuration management tools to detect and automatically correct deviations from its baseline configuration and collects and secures audit records.	Inspected status.moengage.com site for tracking Client SLA.	No exceptions noted.
CCC-08	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	MoEngage maintains configuration management tools to detect and automatically correct deviations from its baseline configuration and collects and secures audit records.	Inspected Jira tool report and sample change tickets.	No exceptions noted.
CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	MoEngage has processes in place to roll back changes or manage operational impact in case the changes have an adverse impact on the production environment.	Inspected Jira tool report and sample change tickets.	No exceptions noted.
Cryptography, Encryption & Key Management- CEK				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure. MoEngage uses AWS KMS.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure. MoEngage key management operates as a service for engineering teams to use in their application code.	Inspected Data Encryption and key management procedure and screenshot showing access to KMS for Mongo.	No exceptions noted.
CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure. MoEngage uses a combination of open source and proprietary encryption formats and algorithms validated by security engineers.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected disk encryption screenshot.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	MoEngage has a robust change management process and security policy that is documented and requires approvals from relevant stakeholders before being released into production.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected sample ticket for accessing keys.	No exceptions noted.
CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	MoEngage has a robust change management process and security policy that is documented and requires approvals from relevant stakeholders before being released into production.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	MoEngage performs a risk assessment for its offerings and the supporting infrastructure in which assets are identified and threats, vulnerabilities, impact, and likelihood are assessed.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	MoEngage provides capabilities to encrypt data by tenant for a subset of products. Customers can manage their own encryption keys on Cloud using Cloud Key Management Services.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	MoEngage uses a proprietary Key Management Service to manage the distribution, generation and rotation of cryptographic keys.	Inspected audit report.	No exceptions noted.
CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	MoEngage uses Key Management Service for storage of cryptographic keys and secrets.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	MoEngage has established policies and procedures that govern the use of cryptographic controls and established key management processes using Data Encryption and key management procedure.	Inspected screenshots related to encryption enablement and key management throughout the key lifecycle. Inspected AWS KMS screenshots.	No exceptions noted.
Datacenter Security- DCS				
DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	NA.	NA.	NA.
DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	NA.	NA.	NA.
DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	NA.	NA.	NA.
DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	NA.	NA.	NA.
DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	NA.	NA.	NA.
DCS-08	Use equipment identification as a method for connection authentication.	NA.	NA.	NA.
DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	NA.	NA.	NA.
DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	NA.	NA.	NA.
DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	NA.	NA.	NA.
DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	NA.	NA.	NA.
DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	NA.	NA.	NA.
DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	NA.	NA.	NA.
Data Security & Privacy Lifecycle Management- DSP				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed Information Classification Policy and Procedure, Information Security Policy and Data retention and protection Policy.	Inspected asset inventory list.	No exceptions noted.
DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	MoEngage has defined documented and reviewed Information Classification Policy and Procedure, Information Security Policy and Data retention and protection Policy.	MoEngage confirmed that AWS manages this requirement.	No exceptions noted.
DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	MoEngage has defined documented and reviewed Information Classification Policy and Procedure, Information Security Policy and Data retention and protection Policy.	Inspected asset inventory list.	No exceptions noted.
DSP-04	Classify data according to its type and sensitivity level.	MoEngage has defined documented and reviewed Information Classification Policy and Procedure, Information Security Policy and Data retention and protection Policy.	Inspected asset inventory list.	No exceptions noted.
DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	MoEngage has defined documented and reviewed Information Classification Policy and Procedure, Information Security Policy and Data retention and protection Policy.	Inspected asset inventory list.	No exceptions noted.
DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	MoEngage has defined documented and reviewed Information Classification Policy and Procedure, Information Security Policy and Data retention and protection Policy.	Inspected security objectives of MoEngage.	No exceptions noted.
DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	NA.	NA.	NA.
DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	NA.	NA.	NA.
DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	NA.	NA.	NA.
DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	NA.	NA.	NA.
DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	NA.	NA.	NA.
DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	NA.	NA.	NA.
DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	NA.	NA.	NA.
DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	NA.	NA.	NA.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	NA.	NA.	NA.
DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	NA.	NA.	NA.
Governance, Risk & Compliance- GRC				
GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	MoEngage defined, documented, implemented, and monitored ISMS. All ISMS documents are reviewed annually.	Inspected organization chart, job descriptions, training records, Risk register, sample communication mails, audit reports, and corrective action reports.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	MoEngage defined, documented, implemented, and monitored ISMS.	Inspected ISMS Scope, Risk register, Job description, performance review reports, backup restoration test screenshots, and DR test plan and reports.	No exceptions noted.
GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	MoEngage reviews its ISMS documentation and security policies annually.	Inspected sample ISMS policies and procedures with revision and review details.	No exceptions noted.
GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	MoEngage has documented its exception processing as part of its information security policy.	Inspected risk register. Inquired the MoEngage management team to understand any deviation cases identified. The management team confirmed that there are no such cases.	No exceptions noted.
GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	MoEngage has defined and documented Information Security Management System. which caters to CCM controls requirements.	Inspected audit report.	No exceptions noted.
GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	MoEngage has defined and documented Information Security Management System.	Inspected organization chart, job description, signed NDA from employees, vendors, background verification reports, training records, audit report and metrics and measurements.	MoEngage needs to be more proactive in assessing metrics and measurements related to ISMS.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	MoEngage has defined and documented Information Security Management System.	Inspected risk register, audit report.	No exceptions noted.
GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	MoEngage maintains contact with the security community and special interest groups documented as part of the Information Security policy.	Inquired management about their contact with special interest groups related to the security domain. They confirmed that they are subscribed to leading security groups.	No exceptions noted.
Human Resources- HRS				
HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	MoEngage has defined and documented policies related to Human Resources related to pre-employment, during employment and post employment.	Inspected background verification reports, and risk registers.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	MoEngage has established an acceptable usage policy that describes acceptable use expectations of MoEngage owned and managed assets. Review is happening on an annual basis.	Inspected risk register, job descriptions, performance review reports, and sample communication mails.	No exceptions noted.
HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	MoEngage has established formal security policies that require all personnel to not leave sensitive materials unattended documented in the acceptable use policy.	Inspected sample communication mails and risk register and training records.	No exceptions noted.
HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	MoEngage has policies in place for working remotely security guidelines which detail the required security and privacy practices for protecting the data while working remotely in information security policy.	Inspected sample communication mails, risk register, user list for access provisioning, Okta screenshot for access provisioning, encryption enablement for protecting Information, cloud screenshot for monitoring.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	MoEngage has a well defined exit process including equipment return procedures for terminated personnel. Exit checklists are provided to both personnel and their managers to inform them of their obligations for returning organizationally-owned assets. Documented in the Employee handbook.	Inspected employee exit checklist for terminated employees.	No exceptions noted.
HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	MoEngage has defined and documented the relocation policy as part of the employee handbook.	Inspected sample communication mails and job descriptions.	No exceptions noted.
HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	MoEngage employees are required to complete the Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information and assets. Employees signs NDA also as part of onboarding process.	Inspected employee acknowledgment of policies and procedures, signed NDA by employees, vendors, contractors and risk register.	No exceptions noted.
HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	MoEngage employees are required to complete the Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information and assets. Employees signs NDA also as part of onboarding process.	Inspected employee acknowledgment of policies and procedures, signed NDA by employees, vendors, contractors and training records.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	MoEngage employees are required to complete the Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information and assets. Employees signs NDA also as part of onboarding process.	Inspected job description, sample communication mails with roles and responsibilities.	No exceptions noted.
HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	MoEngage employees are required to complete the Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information and assets. Employees signs NDA also as part of onboarding process.	Inspected signed NDA by employees and vendors.	No exceptions noted.
HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	MoEngage has defined and documented Security Awareness Training Policy and are reviewed annually.	Inspected sample communication mails, training records and policies acknowledgment, signed mutual NDA by vendors, vendor performance evaluation reports.	No exceptions noted.
HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	MoEngage has defined and documented a security awareness training policy. All employees attend the training program during their onboarding process.	Inspected training records and policies acknowledgement and signed NDA by employees.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	MoEngage has defined and documented a security awareness training policy. All employees attend the training program during their onboarding process.	Inspected job descriptions, sample communication mails.	No exceptions noted.
Identity & Access Management- IAM				
IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected risk register, screenshots for access provision, access revocation and access review confirmation.	No exceptions noted.
IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	MoEngage has defined and documented Password Policy reviewed on annual basis.	Inspected screenshot showing the password policy configured for enforce setting password, usage of complex password, age, history and failed attempts.	No exceptions noted.
IAM-03	Manage, store, and review the information of system identities, and level of access.	MoEngage maintains a central identity and authorization management system.	Inspected screenshot showing request for access provision, revocation and review. Inspected user provision and revocation list.	No exceptions noted.
IAM-04	Employ the separation of duties principle when implementing information system access.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected request approval process for access provision and revocation.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IAM-05	Employ the least privilege principle when implementing information system access.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected request approval screenshot for access provision, revocation and review confirmation.	No exceptions noted.
IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected request approval screenshot for access provision, revocation and review confirmation. Inspected Jira tool reports.	No exceptions noted.
IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected request approval screenshot for access provision, revocation, and review confirmation. Inspected Jira tool reports. inspected user access revocation list.	No exceptions noted.
IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	MoEngage maintains a central identity and authorization management system.	Inspected request approval screenshot for access provision, revocation, and review confirmation and risk register.	No exceptions noted.
IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	MoEngage has defined and documented Information Security policy reviewed on annual basis.	Inspected screenshot showing different groups and roles defined for segregation of duties.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	MoEngage has defined and documented Information Security policy reviewed on annual basis.	Inspected request approval screenshot for access provision, revocation, and review confirmation.	No exceptions noted.
IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected request approval screenshot for access provision, revocation, and review confirmation and risk register.	No exceptions noted.
IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	MoEngage ensures access to audit management information is restricted from unauthorized access through the log repository. Access to logging infrastructure is limited to authorized employees only. Access may vary by levels and must be approved by the reporting manager.	Inspected screenshot showing log management access provided only to restricted personnel.	No exceptions noted.
IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	MoEngage has processes to ensure new employees (including vendors, contractors, and temporary employees) are assigned a username to uniquely identify an individual.	Inspected user creation list and deletion list.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	MoEngage has defined and documented Access Management Policy and procedure reviewed on annual basis.	Inspected request approval screenshot for access provision, revocation, and review confirmation. Inspected MFA enablement screenshot.	No exceptions noted.
IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	MoEngage has defined and documented Policies related to the secure use of passwords as part of password policy.	Inspected screenshot showing password policy Implementation for secured management of passwords.	No exceptions noted.
IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	MoEngage restricts access based on need-to-know and job function by implementing an access management policy.	Inspected request approval screenshot for access provision, revocation, and review confirmation. Inspected user list for creation and revocation.	No exceptions noted.
Interoperability & Portability- IPY				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually	MoEngage has a defined documented and approved Risk Management Policy which covers all application security, Cloud Security risks, and API Risks. Details regarding MoEngage API list can be found on the MoEngage website at: https://developers.moengage.com/hc/en-us https://help.moengage.com/hc/en-us.	Inspected Risk management Policy, Procedure, Risk register, and MoEngage developer's website.	No exceptions noted.
IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	MoEngage provides capabilities to CSC for programmatically retrieving their data to enable interoperability and portability.	Inspected screenshot showing the programmatic way of exporting campaign data using the Open Analytics tool.	No exceptions noted.
IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	MoEngage APIs and MoEngage Management Console are available via TLS-protected endpoints, which provide server authentication.	Inspected screenshots showing the configuration for data export with a secret key used for authentication.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	MoEngage's Data Processing and Security Terms define deletion on termination and data export agreements.	Inspected DPA agreement with all required clauses.	No exceptions noted.
Infrastructure & Virtualization Security- IVS				
IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines.	Inspected risk register covering risks related to cloud Infrastructure, application, audit reports, performance review reports.	No exceptions noted.
IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines.	Inspected auto scaling enablement screenshot.	No exceptions noted.
IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines.	Inspected screenshot for access provisioning request, revocation request and review confirmation, encryption enablement for secured communication, MFA enablement for authentication and authorization and DLP enablement.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines.	Inspected CIS benchmark checklist for hardening various OS and configuration dashboard screenshots.	No exceptions noted.
IVS-05	Separate production and non-production environments.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines. MoEngage has a segregated environment for Production and Non-Production activities.	Inspected SAAS Infrastructure Security Guidelines, screenshot showing SaaS network diagram.	No exceptions noted.
IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines. Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customer data is logically segregated by domain to allow data to be produced for a single tenant.	Inspected SAAS Infrastructure Security Guidelines, SaaS environment diagram.	No exceptions noted.
IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines. MoEngage's encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by MoEngage or on behalf of MoEngage.	Inspected SAAS Infrastructure Security Guidelines, SaaS environment diagram.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
IVS-08	Identify and document high-risk environments.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines. Within MoEngage's production environment, there are high trust environments considered to as privileged access environments and enforced by access controls.	Inspected SAAS Infrastructure Security Guidelines, SaaS environment diagram and risk register.	No exceptions noted.
IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	MoEngage has defined documented and reviewed SAAS Infrastructure Security Guidelines. MoEngage intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents.	Inspected cloud alerts screenshots and events list.	No exceptions noted.
Logging & Monitoring- LOG				
LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	MoEngage has defined and documented and reviewed process for logging and monitoring as part of information security policy.	Inspected screenshot showing logging and monitoring enablement. Inspected sample monitoring alerts and events list.	No exceptions noted.
LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	MoEngage has defined and documented and reviewed process for data retention and protection as part of data retention and protection policy.	Inspected screenshot showing logging and monitoring enablement. Inspected sample monitoring alerts and events list.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	MoEngage has implemented AWS Audit, VPC Cloud, Kavach, and the Deepfence tool for automatic alerting.	Inspected screenshots for Audit, VPC Cloud, Kavach, and Deepfence tool.	No exceptions noted.
LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	MoEngage has defined and documented and reviewed process for logging and monitoring as part of information security policy.	Inspected screenshot showing access to logs Is provided only to restricted and authorized personnel.	No exceptions noted.
LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	MoEngage has defined and documented and reviewed process for logging and monitoring as part of information security policy.	Inspected screenshots for Audit, VPC Cloud, Kavach and the Deepfence.	No exceptions noted.
LOG-06	Use a reliable time source across all relevant information processing systems.	MoEngage has defined and documented Clock Synchronization as part of Information Security Policy.	MoEngage uses the default AWS NTP server for clock synchronization. Inspected screenshot showing the configuration of AWS NTP.	No exceptions noted.
LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	MoEngage has defined and documented and reviewed process for logging and monitoring as part of information security policy.	Inspected screenshot showing log storage and monitoring.	No exceptions noted.
LOG-08	Generate audit records containing relevant security information.	MoEngage has implemented AWS Audit.	Inspected screenshots for AWS Audit.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	MoEngage has defined and documented and reviewed information security policy.	Inspected screenshot showing log access only to authorized personnel only.	No exceptions noted.
LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	MoEngage maintains documentation for the use of its internal key management service is documented in MoEngage SaaS Infrastructure Security Controls & Processes.	Inspected encryption, MFA enablement, AWS KMS throughout key lifecycle screenshots.	No exceptions noted.
LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	MoEngage uses AWS KMS for key management and is defined, documented and reviewed as part of the Data Encryption and key management procedure.	Inspected encryption, MFA enablement, AWS KMS throughout key lifecycle screenshots.	No exceptions noted.
LOG-12	Monitor and log physical access using an auditable access control system.	MoEngage uses AWS for hosting their application and physical security is handled by AWS.	NA.	NA.
LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	MoEngage has defined and documented and reviewed information security policy.	Inspected sample cloud alerts and events list.	No exceptions noted.
Security Incident Management, E-Discovery & Cloud Forensics- SEF				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed IT Security Incident Response Plan and Information Security Policy.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.
SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed IT Security Incident Response Plan and Information Security Policy.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.
SEF-03	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.	MoEngage has defined documented and reviewed IT Security Incident Response Plan and Information Security Policy.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.
SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	MoEngage performs annual testing of its emergency response processes. In addition, MoEngage is proactively managing incidents via OneTrust Portal.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
SEF-05	Establish and monitor information security incident metrics.	MoEngage reviews and analyzes security incidents to determine impact, cause, and opportunities for corrective action. in addition, Incident metrics are collected and monitored in Metrics Dashboard.	Inspected incident report, and root cause analysis tracker.	No exceptions noted.
SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	MoEngage maintains processes for the Incident Management team to triage identified risks or security events/incidents.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.
SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	MoEngage has defined documented and reviewed IT Security Incident Response Plan and Information Security Policy.	Inspected IT Security Incident Response Plan and Information Security Policy and sample incident report.	No exceptions noted.
SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	MoEngage has defined documented and reviewed IT Security Incident Response Plan and Information Security Policy.	Inspected incident review report and contact information as part of the incident response plan document.	No exceptions noted.
Supply chain Management, Transparency & Accountability- STA				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed SAAS infrastructure security guidelines and SSRM document.	Inspected signed agreements with suppliers providing all security requirements and supplier evaluation reports.	No exceptions noted.
STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	MoEngage has defined documented and reviewed SAAS infrastructure security guidelines and SSRM document covering suppliers.	Inspected signed agreements with suppliers providing all security requirements and supplier evaluation reports.	No exceptions noted.
STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	MoEngage has defined documented and reviewed SAAS infrastructure security guidelines and SSRM document.	Inspected signed agreements with the clients providing all security requirements.	No exceptions noted.
STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	MoEngage has defined documented and reviewed SAAS infrastructure security guidelines and SSRM document.	Inspected signed DPA agreement covering all data and security requirements.	No exceptions noted.
STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	MoEngage has defined documented and reviewed SAAS infrastructure security guidelines and SSRM document.	Inspected signed DPA agreement covering all data and security requirements.	No exceptions noted.
STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	MoEngage has defined documented and reviewed SAAS infrastructure security guidelines and SSRM document.	Inspected signed DPA agreement covering all data and security requirements and supplier evaluation reports.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
STA-07	Develop and maintain an inventory of all supply chain relationships.	MoEngage has defined documented and reviewed supplier relationship management policy.	Inspected vendor security review document with all supplier details.	No exceptions noted.
STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	MoEngage has defined and documented and reviewed risk management policy and procedure covering third party risks.	Inspected risk register covering third party risks.	No exceptions noted.
STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	MoEngage has defined documented and reviewed supplier relationship management policy.	Inspected sample signed DPA agreements covering all the requirements.	No exceptions noted.
STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	MoEngage has defined documented and reviewed supplier relationship management policy.	Inspected Vendor security review document with all supplier details.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	MoEngage has defined documented and reviewed supplier relationship management policy which covers monitoring and review of supplier services.	Inspected vendor security review report.	No exceptions noted.
STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	MoEngage has defined documented and reviewed supplier relationship management policy which covers monitoring and review of supplier services.	Inspected vendor security review report.	No exceptions noted.
STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	MoEngage has defined documented and reviewed supplier relationship management policy which covers monitoring and review of supplier services.	Inspected vendor security review report.	No exceptions noted.
STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	MoEngage has defined documented and reviewed supplier relationship management policy which covers monitoring and review of supplier services.	Inspected vendor security review report.	No exceptions noted.
Threat & Vulnerability Management- TVM				

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed vulnerability management procedure.	Inspected VAPT report.	No exceptions noted.
TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed antivirus policy and procedure. MoEngage Systems are scanned for any virus/malware.	Inspected Sophos Central Dashboard Screenshots.	No exceptions noted.
TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	MoEngage has defined documented and reviewed vulnerability management procedure.	Inspected VAPT report.	No exceptions noted.
TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	MoEngage has defined documented and reviewed vulnerability management procedure.	Inspected VAPT report.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	MoEngage has defined documented and reviewed vulnerability management procedure.	Inspected VAPT report.	No exceptions noted.
TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	MoEngage has defined documented and reviewed vulnerability management procedure.	Inspected VAPT report.	No exceptions noted.
TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	MoEngage has defined documented and reviewed vulnerability management procedure. Conducts internal scan quarterly and penetration testing annually or whenever any changes to the application.	Inspected VAPT report.	No exceptions noted.
TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	MoEngage has defined documented and reviewed vulnerability management procedure. Conducts internal scan quarterly and penetration testing annually or whenever any changes to the application.	Inspected VAPT report.	No exceptions noted.
TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	MoEngage has defined documented and reviewed vulnerability management procedure. Conducts internal scan quarterly and penetration testing annually or whenever any changes to the application.	Inspected VAPT report.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	MoEngage has defined documented and reviewed vulnerability management procedure. Conducts internal scan quarterly and penetration testing annually or whenever any changes to the application.	Inspected VAPT report and Vulnerabilities list.	No exceptions noted.
Universal Endpoint Management- UEM				
UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	MoEngage has defined documented and reviewed information security policy for security requirements owned and managed endpoints.	Inspected Deepfence configuration, MFA enablement, disk encryption enablement screenshots.	No exceptions noted.
UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	MoEngage has defined documented and reviewed information security policy for security requirements owned and managed endpoints.	Inspected software list.	No exceptions noted.
UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	MoEngage has defined documented and reviewed information security policy for security requirements owned and managed endpoints.	Inspected Deepfence screenshots.	No exceptions noted.
UEM-04	Maintain an inventory of all endpoints used to store and access company data.	MoEngage maintains a centralized inventory system for all managed endpoints.	Inspected asset inventory list.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	MoEngage has implemented technical measures in which all devices must have a trust tier designation. Each trust tier allows varying levels of access to corporate systems.	Inspected screenshot showing the users and organizations configured.	No exceptions noted.
UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	MoEngage requires that all devices must implement an automatic screen lock after a pre-defined period of time.	Inspected automatic lock screen configuration screenshot.	No exceptions noted.
UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	MoEngage endpoint devices are continuously patched through system management software as patches become available, which varies by OS and applications. Documented in Change management Policy.	Inspected risk register, Jira tool reports and SLA reports, patches deployed report.	No exceptions noted.
UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	MoEngage requires all managed endpoints to be encrypted during the initial setup process and remain encrypted throughout the device's lifecycle.	Inspected disk encryption enablement screenshot.	No exceptions noted.
UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	MoEngage has mechanisms in which IT team issued machines have antivirus software preinstalled to help prevent, detect, and remove malware, depending on the OS. Antivirus Policy is in place.	Inspected Sophos central dashboard.	No exceptions noted.

CCM #	CCM Controls Description	Description & Design of Controls	Evaluation of Controls	Remarks
UEM-10	Configure managed endpoints with properly configured software firewalls.	MoEngage manages Mac, and Windows, computers have personal firewalls enabled and managed by an internal team.	Inspected personal firewall enablement screenshot.	No exceptions noted.
UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	MoEngage leverages the MoEngage Workspace DLP functionalities.	Inspected DLP enablement screenshot.	No exceptions noted.
UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	MoEngage has mechanisms in place to provide recent physical locations for employees based on corporate activity logs. This system is used for location-based access restrictions.	Inspected sample logs.	No exceptions noted.
UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	MoEngage has policies and procedures in place for mobile device security guidelines which state MoEngage reserves the right to remotely wipe mobile devices. In addition to remote wipe capabilities, MoEngage uses strong encryption modules on all highly privileged access mobile devices.	Inspected screenshot showing wipe computer to enable the deletion of company data remotely on managed endpoint devices.	No exceptions noted.
UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	MoEngage does not utilize third-party contractors to provide services to customers and involved them in any activity requiring access to MoEngage Customer Data.	NA.	NA.

End of document