Service Organization Control 3 (SOC 3®) Type 2 Report

Gradient MSP Inc.'s report on its Platform relevant to Security, Confidentiality and Privacy for the period October 1, 2021 to September 30, 2022

mhm professional corporation
CHARTERED PROFESSIONAL ACCOUNTANT

Table of Contents

Section I

Gradient MSP Inc.'s Management Assertion

Gradient MSP Inc.’s Management Assertion

We are responsible for designing, implementing, operating and maintaining effective controls within Gradient MSP Inc.’s (“Gradient”) Platform (“system”) throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Gradient MSP Inc.’s service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Gradient MSP Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality and privacy (“applicable trust services criteria”) set forth in TSP Section 100, 2017 Trust Services Criteria for security, confidentiality and privacy, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Gradient MSP Inc.’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Gradient MSP Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
Colin Knox
19C1305AF1C249F...

Colin Knox, CEO
Gradient MSP Inc.
October 31, 2022

Section II

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Gradient MSP Inc.:

Scope

We have examined Gradient MSP Inc.'s ("Gradient") accompanying assertion titled "Gradient MSP Inc.'s Management Assertion" ("assertion") that the controls within the Gradient MSP Inc. Platform ("system") were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Gradient MSP Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for security, confidentiality and privacy, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service organization's responsibilities

Gradient MSP Inc. is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that Gradient's service commitments and system requirements were achieved. In Section I, Gradient has provided the accompanying assertion titled "Management of Gradient MSP Inc.'s Assertion" ("assertion"), about the effectiveness of controls within the system. When preparing its assertion, Gradient MSP Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditors' responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with the Canadian

Standard on Assurance Engagements 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance* and with attestation standards established by the American Institute of Certified Public Accountants (AICPA). These standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Gradient's service commitments and system requirements based on the applicable trust criteria.
- Performing such other procedures as we considered necessary in the circumstances

Inherent limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the Gradient MSP Inc. Platform were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Gradient's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated in all material respects.

Restricted use

Certain complementary subservice controls that are suitably designed and operating effectively are necessary, along with controls at Gradient MSP Inc., to achieve Gradient MSP Inc.'s service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Gradient MSP Inc. uses Amazon Web Services to provide cloud infrastructure services. Users of this report should obtain the relevant Amazon Web Services SOC2 or SOC3 report.

DocuSigned by:
MHM Professional Corporation
4F227774372B4BC...

Chartered Professional Accountant
Calgary, Alberta
October 31, 2022

Attachment A

Gradient MSP Inc.’s Description of the Boundaries of its Platform

Gradient MSP Inc.'s Description of the Boundaries of its Platform

Company Overview

Gradient MSP Inc. is a privately held technology company founded in 2020 and headquartered in Calgary, Alberta. Gradient MSP Inc. provides the Gradient Platform for small business to enterprise. The Gradient Platform provides services to support the operations of IT Service Professionals and the vendors that serve them. It includes, but is not limited to, a data hygiene analysis tool that connects with a customer's Professional Services Automation software (PSA) and enables them to easily review recommendations and update those records directly in their PSA for remediation and a billing reconciliation tool that connects with the customer's PSA and vendor billing records to automatically update contracts resulting in timely and accurate client invoicing.

Services Provided

Gradient provides services to ingest and review Professional Services Automation (PSA) software data connected through that software's API and provides recommendations on the validity of that data. It enables users to act on those recommendations by approving a remediation action that will take place directly in their PSA. The Gradient Platform is a SaaS solution that includes a web-based user interface for these services. Customers can see the overall validity of their data through a dashboard demonstrating potential cost savings and revenue opportunities and the values change as they continue to act on the recommendations of the solution.

The Boundaries of the System Used to Provide the Services

The boundaries of the system are the specific aspects of Gradient MSP Inc.'s infrastructure, software, people, procedures and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly supports the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as described in the sections below.

Infrastructure

Gradient Platform is a SaaS-multi-tenant client-server application hosted in Amazon Web Services. Each tenant on the Gradient Platform is logically separated by organization and not accessible to other organizations to prevent unauthorized access.

The Gradient application runs within an AWS VPC using the us-east-2 region and utilizes two Availability Zones, us-east-2a and us-east-2b. The application runs on a t3.large instance, running Amazon Linux 2 as the operating system. It is one application structure with the backend API written in Node.JS and the frontend written in Javascript React.JS. ExpressJS is utilized as the web server with NGINX.

The database supporting the application is managed by Atlas utilizing AWS cloud infrastructure running MongoDB. The primary database is replicated real time into secondary and tertiary databases in the primary region for backup and redundancy purposes. AWS ElastiCache Redis is used for job queue state management. AWS CloudWatch is used for both monitoring and log storage. Customer data is also transformed and uploaded into a data lake hosted by Snowflake on AWS for analysis purposes.

Software

The following provides a summary of software systems used to deliver Gradient Platform:

- AWS CloudWatch – used for the monitoring of production systems, log storage availability and capacity.
- AWS GuardDuty – used for web application vulnerability scanning.
- GitHub – used for source code version control.
- Amazon Linux 2– operating systems to support operation of the system.
- Node.JS – programming language used to write the backend API of the web application.
- Sendgrid - used for sending application email

People

Gradient has a defined organizational structure with specific roles, responsibilities, and appropriate lines of reporting required to support the Gradient Platform. It is comprised of, and supported by, the following teams who are responsible for the delivery and management of the system:

- Executive – responsible for providing the overall direction, strategic vision, and management of Gradient.
- Product – responsible for guiding the overall direction of the product roadmap including usability, enhancements, and new features.
- Engineering – responsible for front and back-end development of the in-scope applications and services. Also, responsible for oversight of software and data engineering, IT Infrastructure, and all IT related activities.
- Operations – responsible for day-to-day operations, such as document processing and office functions.
- Marketing – responsible for generating leads and promoting Gradient Platform to the market
- Sales – responsible for development of new business related to the Gradient services.
- Partner Success - responsible for successful onboarding of customers on Gradient Platform and act as advocates for the continued success of the platform. Partner Success is also responsible for product support issues, customer engagement and growth.

The teams and associated initiatives, workstreams, and functions are led by the executive management leads.

Policies, Processes & Procedures

Management has developed and communicated to employees and contractors a set of policies, processes, and procedures in several operational areas which support the security, privacy, and confidentiality objectives of the Platform. As part of the wider Information Security Management Program, Gradient has developed and organized the following policies and procedure documents that are used to support the Platform.

The following policies and procedures are available to employees and contractors through the Platform:

- Acceptable Use
- Access Control
- Backup and Restoration
- Business Continuity and Disaster Recovery
- Change Management
- Corporate Ethics
- Customer Support and SLA
- Data Retention and Disposal
- Incident Management
- Information Classification
- Information Security
- Internal Audit
- IT Asset Management
- Key Management and Cryptography
- Mobile Device Management
- Network Security
- Personnel Security
- Privacy Policy for Websites
- Risk Assessment
- Server Security
- Software Development
- Vendor Management
- Vulnerability Management
- Workstation Security

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. Gradient has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

Data is entered via the client web application (React.JS), and sent to the application servers via REST calls to the API. The data is processed and written to the Atlas database cluster. Data transmission is secured using TLS 1.2, SHA-256 with RS 2048 Encryption, and does not leave the VPC. Data replication channels are also encrypted and transmitted via the private AWS connection. All data access requests require an ACL context which contains both the authenticated user and the organization that is requesting the data. These requests are validated via the Gradient MSP Inc. permissions system to exclude the possibility of cross-client data leakage. All data at rest is encrypted using Advanced Encryption Standard encryption.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Gradient designs its processes and procedures related to its Platform to meet its objectives. Those objectives are based on the service commitments that Gradient makes to user entities, regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Gradient has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the Platform that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.

Confidentiality commitments to user entities are documented in client agreements. Confidentiality commitments are standardized and include, but are not limited to, the following:

- Information is defined and classified into categories with associated retention periods.
- Data retention and disposal policies and procedures are documented and in place.

Privacy commitments to user entities are documented in client agreements. Privacy commitments are standardized and include, but are not limited to, the following:

- Maintaining a privacy officer and privacy policy accessible to clients.
- Restricting access to personal information for only necessary purposes.
- Responding to data requests and notification of data breaches in a timely manner.
- Establishing a process for disclosing personal information to third parties.
- Gradient does not and will not sell client’s and their customers’ information. Gradient does not share or disclose data to third parties for their advertising purposes.

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