

SOC 2[®] TYPE 2 REPORT ON CONTROLS RELEVANT TO
SECURITY FOR PATIENT SUCCESS PLATFORM SERVICES

LUMA HEALTH, INC.

MAY 1, 2024 TO APRIL 30, 2025



LUMA HEALTH, INC.

Table of Contents

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2: MANAGEMENT'S ASSERTION	5
SECTION 3: DESCRIPTION OF THE SYSTEM	7
SCOPE OF REPORT AND DISCLOSURES	8
Overview	8
Trust Services Categories and Related Criteria	8
Scope	9
Sub-Service Organizations	10
Significant Changes during the Examination Period	10
Subsequent Events	10
System Incidents	10
Using the Work of the Internal Audit Function	10
OVERVIEW OF OPERATIONS AND THE SYSTEM	11
Company Overview and Background	11
Overview of the Patient Success Platform Services System	11
Principal Service Commitments and System Requirements	11
Infrastructure	13
Software	13
People	14
Procedures	15
Data	18
RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, AND MONITORING	19
Control Environment	19
Risk Assessment	21
Information and Communication Systems	23
Monitoring	24
CATEGORIES, CRITERIA, AND RELATED CONTROLS	26
COMPLEMENTARY CONTROL CONSIDERATIONS	27
SECTION 4: CATEGORIES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS	28
INFORMATION PROVIDED BY THE SERVICE AUDITOR	29
Introduction	29
Tests of Operating Effectiveness	29
Types of Tests Performed	30
Procedures for Assessing Completeness and Accuracy of IPE	30
Sampling Methodology	31
CATEGORIES, CRITERIA, AND RELATED CONTROLS	32
Security (Common Criteria to All Categories)	32

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Luma Health, Inc.:

Scope

We have examined the accompanying description of Luma Health, Inc.'s ("Luma") Patient Success Platform Services system throughout the period May 1, 2024 to April 30, 2025, based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Luma's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Luma uses Amazon Web Services, Inc., MongoDB, Inc., and Google, LLC, sub-service organizations, for cloud hosting and managed services, managed database services, and user authentication and credentialing services, respectively. The description indicates that complementary sub-service organization controls that are suitably designed and operating effectively are necessary, along with controls at Luma, to achieve Luma's service commitments and system requirements based on the applicable trust services criteria. The description presents Luma's controls, the applicable trust services criteria, and the types of complementary sub-service organization controls assumed in the design of Luma's controls. The description does not disclose the actual controls at the sub-service organizations. Our examination did not include the services provided by the sub-service organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary sub-service organization controls.

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of this report.

Opinion

In our opinion, in all material respects:

- a. the description presents Luma's Patient Success Platform Services system that was designed and implemented throughout the period May 1, 2024 to April 30, 2025, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Luma's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the sub-service organizations and user entities applied the complementary controls, if applicable, assumed in the design of Luma's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Luma's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary sub-service organization and complementary user entity controls, if applicable, assumed in the design of Luma's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Luma, user entities of Luma's Patient Success Platform Services system during some or all of the period May 1, 2024 to April 30, 2025, business partners of Luma subject to risks arising from interactions with the Patient Success Platform Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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



July 10, 2025
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT OF LUMA HEALTH, INC.'S ASSERTION

July 10, 2025

We have prepared the accompanying description of Luma Health, Inc.'s ("Luma") Patient Success Platform Services system throughout the period May 1, 2024 to April 30, 2025, based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Patient Success Platform Services system that may be useful when assessing the risks arising from interactions with Luma's system, particularly information about system controls that Luma has designed, implemented, and operated to provide reasonable assurance that our service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Luma Amazon Web Services, Inc., MongoDB, Inc., and Google, LLC, sub-service organizations, for cloud hosting and managed services, managed database services, and user authentication and credentialing services, respectively. The description indicates that complementary sub-service organization controls that are suitably designed and operating effectively are necessary, along with controls at Luma, to achieve Luma's service commitments and system requirements based on the applicable trust services criteria. The description presents Luma's controls, the applicable trust services criteria, and the types of complementary sub-service organization controls assumed in the design of Luma's controls. The description does not disclose the actual controls at the sub-service organizations.

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

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

- a. the description presents Luma's Patient Success Platform Services system that was designed and implemented throughout the period May 1, 2024 to April 30, 2025, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Luma's service commitments and system requirements would be achieved based on the applicable trust services criteria, if our controls operated effectively throughout the period, and if the sub-service organizations and user entities applied the complementary controls, if applicable, assumed in the design of Luma's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Luma's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary sub-service organization controls and complementary user entity controls, if applicable, assumed in the design of Luma's controls operated effectively throughout that period.

/s/ Luma Health, Inc.

Nick Lees – Director of Information Security and Compliance

SECTION 3:

DESCRIPTION OF THE SYSTEM

SCOPE OF REPORT AND DISCLOSURES

Overview

This description of the system of controls provided by Luma Health, Inc.'s ("Luma") management, as related to Statement on Standards for Attestation Engagements No. 21 '*Direct Examination Engagements*', specifically AT-C Section 105, '*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Assertion – Based Examination Engagements*,' considers the direct and indirect impact of risks and controls that Luma's management has determined are likely to be relevant to its user entities' internal controls intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy.

Trust Services Categories and Related Criteria

The five attributes of a system are known as *categories*, and they are defined as follows:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Security refers to the protection of

- i. information during its collection or creation, use, processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

- **Availability:** Information and systems are available for operation and use to meet the entity's objectives.

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

- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

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

- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.

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

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

- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

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

The privacy criteria are organized into eight categories:

- a. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.
- b. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- c. *Collection.* The entity collects personal information to meet its objectives related to privacy.
- d. *Use, retention, and disposal.* The entity limits use, retention, and disposal of personal information to meet its objectives related to privacy.
- e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- g. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
- h. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

The trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories, either individually or in combination with controls in other categories.

Scope

The scope that management has determined appropriate for the Patient Success Platform Services system includes the controls to meet the applicable trust services criteria. Management is responsible for the identification of risks associated with the system of controls, and for the design and operation of controls intended to provide reasonable assurance that the applicable trust services criteria would be met.

As part of its overall SOC 2® program, Luma's management sets and determines the scope and timing of each report. This description of the system has been prepared by Luma's management, headquartered in San Mateo, California, to provide information on controls applicable to meet the trust services criteria for Security.

Sub-Service Organizations

Luma uses Amazon Web Services, Inc. (“AWS”), MongoDB, Inc. (“MongoDB”), and Google, LLC (“Google Workspace”), sub-service organizations, for cloud hosting and managed services, managed database services, and user authentication and credentialing services, respectively. The description included in Section 3 of this report does not include the controls of the sub-service organizations. Management obtains and reviews the annual Service Auditor’s reports for the sub-service organizations to monitor and evaluate the adequacy and effectiveness of the controls in place at the sub-service organizations.

Significant Changes during the Examination Period

Management is not aware of any significant changes that occurred during the examination period.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the period covered by management’s description included in Section 3 of this report through the date of the service auditor’s report that would have a significant effect on management’s assertion.

System Incidents

Management is not aware of any system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more service commitments and system requirements during the period covered by management’s description included in Section 3 of this report.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

Luma was founded in 2015 and is headquartered in San Mateo, California. The company provides a Patient Success Platform that allows patients to connect to their healthcare provider in a way that's modern and mobile-first. Currently, Luma's network includes over 500 healthcare organizations across the United States. Luma continues to build and expand its network through various partnerships including the healthcare transportation services such as Uber Health and electronic health record management systems – Allscripts, Epic, Cerner, and CareCloud.

Overview of the Patient Success Platform Services System

The Patient Success Platform Services system is a cloud-based platform which enables web-based clinic visit scheduling, appointment reminders via texts, referral management, and instant communication between clinics and patients. The system aims to drive clinic-patient engagement throughout the patient journey, as follows:

- Self-scheduling and referral management
- Automated waitlists and appointment reminders
- Mobile patient intake by capturing required patient data electronically
- Actionable text messages to improve medication adherence and encourage health behaviors
- Patient communication and feedback

Principal Service Commitments and System Requirements

Luma's management designs its processes and procedures related to the Patient Success Platform Services system to meet its objectives. Those objectives are based on the service commitments that Luma's management makes to user entities; the laws and regulations that govern the provisioning of the Patient Success Platform Services system; and the financial, operational, and compliance requirements that Luma has established for the services.

Luma maintains its IT infrastructure and product offerings through AWS. Therefore, Luma relies on AWS' service commitments related to file backups, retention, business continuity and disaster recovery planning, and availability requirements. Luma identifies AWS as a vendor critical to business operations and reviews AWS' service agreements and relevant third-party assessments on an annual basis to help ensure alignment of commitments to Luma's operational and business objectives.

Luma communicates service commitments and system requirements to customers in written individualized agreements and statements published on its web portal. Customers are required to sign an agreement prior to using Patient Success Platform Services. These commitments generally include the following:

Trust Services Category	Service Commitments	System Requirements
Security	➤ System access is granted to authorized personnel only ➤ Maintain security and integrity of services and content	➤ Account and password management standards ➤ Vulnerability assessment and remediation standards ➤ Workforce vetting and training standards

Trust Services Category	Service Commitments	System Requirements
	➤ Implement appropriate safeguards as are necessary to prevent the use or unauthorized disclosure of PHI ➤ Ensure that vendors whom it provides PHI, agrees to the same restrictions and conditions that apply to Luma with respect to such information ➤ Ensure that vendors whom it provides PHI, agrees to implement reasonable and appropriate safeguards to protect it	➤ System and application change management standards ➤ Encryption standards ➤ Vendor management standards

Such requirements are communicated in Luma's 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, trained, and managed. 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 Patient Success Platform Services system.

OVERVIEW OF RELEVANT INFRASTRUCTURE

The Patient Success Platform Services system is comprised of the following components:

- Infrastructure – the physical structures, information technology (IT), and other hardware
- Software – the application programs and IT system software that supports application programs
- People – the personnel involved in the governance, operation, and use of a system
- Procedures – the automated and manual procedures
- Data – transaction streams, files, databases, tables, and output used or processed by the system

Infrastructure

Luma's production systems are hosted by AWS and the production databases are hosted by MongoDB. In addition, Luma utilizes Google Workspace as a centralized authentication system to authenticate users and provide multi-factor authentication (MFA) to the production environment.

Luma does not own or maintain any of the hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure including physical infrastructure, geographical regions, availability zones, and edge locations. The system deployed in AWS includes customer data, applications, network security group configuration, network traffic, and server-side encryption.

The AWS infrastructure is maintained via the use of infrastructure as code (IaC) technology through Terraform which utilizes scripting to define the baseline configurations that are applied to systems. A Kubernetes-based containerization infrastructure is utilized via Amazon Elastic Kubernetes Service (EKS) to ensure scalability as well.

The following describes the in-scope components supporting the Patient Success Platform Services system:

System / Application	Description	Infrastructure
Patient Success Platform Services	Cloud-based platform which enables web-based clinic visit scheduling, appointment reminders via texts, referral management, and instant communication between clinics and patients.	Amazon Linux Amazon VPC AWS Availability Zones EKS Terraform MongoDB Atlas

Software

Luma's system refers to the guidelines and activities for providing services to user entities and includes the infrastructure and software that support Luma's Patient Success Platform Services system. Users of the application include customers at partnered healthcare providers, patients, and internal Luma personnel. Customers can add, remove, and manage patient accounts and communications.

The software utilized by Luma to achieve daily objectives includes the following:

- Argo CD – Continuous application deployment and workflow tool.
- Mineral – Enterprise human resources (HR) and workforce training platform.

- ClickUp – Project management and ticketing solution used to track system changes and reported incidents.
- Edge Delta – Transaction log monitoring tool for the production databases.
- CrowdStrike – Endpoint detection and response (EDR) system deployed on organizational laptops.
- Jamf Pro – Mobile Device Management (MDM) solution used for managing organizational laptops.
- Grafana Loki – Enterprise log management and monitoring solution used to monitor production systems and resources.
- GitHub – Provider of internet hosting for software and infrastructure development and source code version control.
- Guru – Internal wiki for company procedures.
- Intruder – Cloud-based vulnerability scanner.
- PagerDuty – Incident response and escalation tool.
- Papertrail – Log management solution used to monitor the message queue.
- Sequoia One – Human Resources Information System (HRIS) tool used to track employees.
- RabbitMQ – Open-source message broker used to handle workload from the message queue.
- Salesforce – Web-based platform for providing customer relationship management services.
- Site24x7 – A website, application, and resource monitoring solution.
- Slack – A chat tool used by Luma staff to communicate internally.
- Twilio – An SMS service used to handle and deliver communications between patients and providers.
- WireGuard – VPN solution used to connect to platform resources.

People

Executive Management and Board of Directors – The Executive Management team and Board of Directors are responsible for (1) overseeing company-wide activities; and (2) establishing business and strategic objectives.

HR – The HR department is responsible for (1) establishing employee behavioral policies; (2) acquiring and retaining competent individuals; and (3) monitoring training to maintain and advance skillsets.

IT – The IT team is responsible for monitoring and providing service and support to the information resources throughout the enterprise.

Site Reliability Engineering (SRE) – The SRE team is responsible for (1) monitoring availability and performance of the environment; and (2) the development of the platform and implementing changes to the supporting infrastructure.

Privacy and Security – The Privacy and Security team is responsible for (1) establishing privacy and security policies; (2) performing risk assessments; and (3) monitoring and addressing security issues and incidents throughout the enterprise.

Legal – The Legal department is responsible for providing legal counsel and review on matters pertaining to privacy and security, intellectual property, master service agreements (MSA), non-disclosure agreements (NDA), and statements of work (SOW).

Procedures

Luma's management is responsible for maintaining and implementing IT general computer controls related to computer processing supporting the Patient Success Platform Services system. These controls provide the basis for reliance on information / data from the systems used by user entities.

Physical Security

Luma's Patient Success Platform service is hosted within AWS and MongoDB. Physical access to the facilities and hardware hosting Luma's platform is the responsibility of AWS and MongoDB. Luma monitors the effectiveness of AWS' and MongoDB's physical security controls via inspection of their annual Service Auditor reports on an annual basis.

Information Security

Information security policies have been established to set the overall framework for managing security of IT and supporting applications. These policies are approved at the executive level and establish standards for information security throughout Luma's information resources and are updated on at least an annual basis. Enforcement of violations of the of the information security protocols are documented within the policies. The IT group has primary responsibility for interpreting these standards, developing procedures and processes for implementing the standards, and overseeing logical security for Luma. A policy repository is utilized for storing and accessing organizational information security policies. In addition, IT develops configuration standards for each type of hardware and associated system software.

Access, Authentication, and Authorization

Employees are required to access system resources through their single sign-on credentials, which consist of a unique username and password. Passwords have been configured to enforce minimum length and specific character requirements. Administrator privileges to system resources are restricted to appropriate personnel and are approved and granted based on job responsibilities. The Luma environment resides within the AWS cloud infrastructure. Administrative access to systems and infrastructure is restricted to personnel commensurate with their job role. Web sessions are encrypted using TLS encryption protocol.

Access Requests and Access Revocation

Each in-scope asset is assigned an owner who is responsible for maintaining access rights. A resource management system is in place to systematically provision and deprovision access to in-scope systems. Asset owners are notified via the resource management system when an employee is hired, so that access privileges to system resources can be granted. Role-based access controls limit employees' system resource access and require explicit approval for access not commensurate with their job role. User access to production systems is reviewed on a semi-annual basis to ensure that access to system resources is appropriately restricted.

An access revocation ticket is completed as a component of the employee termination procedures to document collection of equipment assigned to the employee and revoke systems access. IT administrators are automatically notified through the resource management system when an employee is terminated so that access privileges to system resources can be revoked in a timely manner. A standard deprovisioning checklist is completed as part of the offboarding process.

Mobile Device Management

Luma utilizes MDM tool that provides the capability to remotely wipe devices in the event of loss, theft, or upon user termination. Additionally, this tool assists with enforcing the antivirus tool on all devices that are joined to the tool. The antivirus software is configured on workstations and mobile devices for real-time protection against malware.

Change Management

Management defines documentation and approval requirements based on the change category. Changes to the applications and infrastructure supporting in-scope applications follow a formal change control policy to ensure that only authorized changes are implemented into the production environment. Change control procedures include, but are not limited to, the following:

- Identification and recording of changes;
- Planning and testing of changes prior to implementation into the production environment; validation of input and proper error handling;
- Code review and version control of developed code;
- Assessment of the potential impacts, including security impacts, of such changes;
- Formal approval procedure for proposed changes from application, system, or infrastructure owners; communication of change details to relevant stakeholders;
- Back-out procedures;
- Development and staging environments that are separated from the production environment; and
- Separation of duties between development personnel and those assigned to manage the production environment.

The product development team uses an Agile aligned approach to product delivery, which consists of a hybrid of the Kanban and Scrum frameworks. The development team is divided into smaller units, referred to as pods. Sprint cycles vary in length and are determined by the development pod. At the end of each sprint cycle, pods present their work that was completed in a demo format to the larger development team. Incremental releases, such as, feature updates and bug fixes occur weekly. Product development and feature release efforts occur on a quarterly basis and are expected as part of the business.

Changes are documented and tracked in a ticketing system to ensure review and approval prior to deployment to production and to enable effective coordination and communication between business and developers. Changes are ranked according to their business value and potential impact to the security and functionality of the platform and systems. Change activities are completed in a development environment separated from testing and production environments. Changes are reviewed by at least one other developer prior deployment to the production environment. Once change development activities are completed, the change is pushed to a testing environment for quality assurance (QA) review and approval prior to implementation in the production environment.

In addition, monitoring and alerting tools are in place to detect any potential unauthorized changes to the in-scope systems. A source code repository tool is also utilized to maintain version control on application source codes and restrict development responsibilities to authorized IT personnel.

Incident Response

A security incident response policy is in place to manage unexpected incidents impacting operations and security commitments to customers. The incident response procedures are tested annually to ensure that individuals on the incident response team understand their roles and responsibilities and validate that the procedures in place adequately address potential incidents. The focus of incident management is to minimize downtime, service degradation, or security risk for customers and internal users. System monitoring tools including, but not limited to, environmental sensors, availability tools, and performance monitors are in place to automatically notify IT operations team and IT executives in the event of security incidents. Customers are also notified of any events that may be customer sensitive.

The investigative actions taken are recorded in the incident ticket and document the timing of procedures from discovery to resolution. Any major security incidents resulting in system outages or service disruptions require a post-incident review. The goal of the post-incident review is to establish the root cause and follow-up actions to reduce the risk of repeated incidents. If an incident requires changes in the system, the actions taken in managing an incident are recorded in an incident management system under an incident ticket and follow the standard change management process.

Data Backups

Luma stores customer data in secure clustered databases hosted and managed by MongoDB. Luma has configured multiple iterative backup jobs to prevent data loss due to unforeseen events or disasters. Backups of production databases are encrypted and retained for a minimum of seven years.

Disaster Recovery

A disaster recovery and business continuity plan are in place to guide personnel in procedures to minimize disruptions to the business caused by an unexpected event. The Disaster Recovery strategy combines cloud-based high-availability architecture with defined roles, responsibilities, and procedures if manual intervention is necessary. A test of the disaster recovery plan is conducted annually to ensure the proficiency of personnel and to identify weaknesses in the plan that could hinder recovery in a real emergency.

Data

The data captured in the system includes application access and usage information. Customers have the ability to retrieve reports related to their access and usage activities via the customer portal, where they can also provide feedback and report issues. Significant events and conditions are captured in the system and application logs. Additionally, Luma maintains policies that prohibit the transmission of sensitive information over the Internet or other public communications paths.

Data Classification

Customer data imported, stored, and utilized through deployment of the Patient Success Platform Services system is classified as Confidential. People, applications, infrastructure, and processes with access to confidential data require additional security measures, including role-based access controls and security awareness training.

Data Destruction

Luma leverages virtual disk space with their cloud providers. Data deletion is performed using provided mechanisms covered in their attestations. During the annual vendor assessments, this functionality is validated.

A defined secure customer data deletion policy is maintained by Luma that outlines how long customer data is to be retained upon termination. Luma also provides notice to customers that they will have a seven-day window to request an extract of their data prior to it being deleted. Once the predefined period has passed, customer data is securely deleted from the Luma systems.

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, AND MONITORING

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for the other components of internal controls, providing discipline and structure. Aspects of Luma's control environment that affect the services provided and / or the system of controls are identified in this section.

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are important elements of Luma's control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel engaging in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Employee performance is monitored and rated not only on whether they meet goals and objectives, but on how they meet their objectives. Management emphasizes high standards during its interpersonal communications via meetings, email, and phone calls. Any questionable acts are dealt with promptly and positive acts are recognized and acknowledged in public forums to reinforce positive / constructive behaviors. Employees who violate these standards are disciplined according to a documented employee sanction clause, defining disciplinary action.

Board of Directors and Executive Management

Luma's control consciousness is influenced significantly by its Board of Directors. Attributes include the Board's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management. The Board establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment. The Board of Directors meets on a quarterly basis to oversee the activities of the company regarding organizational strategy, risk, and operations.

Executive Management is responsible for carrying out the strategic plans set by the Board of Directors and meets on a quarterly basis to formulate the deployment of the company's strategic direction, goals, and financial plans for meeting the strategic plan. Past performance on key controls and goals are measured and the results are communicated to various levels of management through meetings and announcements.

Commitment to Competence

Management has established a framework for the basic skills necessary to perform each of the jobs at Luma. Management defines the competence levels for positions and how those levels translate into requisite skills and knowledge through formal job descriptions. Management focuses on hiring experienced employees for the various positions required for the business.

During the interview process, management assesses each job candidate to determine whether they possess the requisite level of competence to hold the position. Newly hired and existing employees are offered opportunities to take training courses that can enhance their skillset and help them to perform their jobs. Functional and administrative job responsibilities are established for key positions and are formally segregated by appropriate function, with management providing leadership and accountability for their respective areas.

Management's Philosophy and Operating Style

Luma's management philosophy and operating style is ultimately responsible for the system of internal controls and encompasses a broad range of characteristics. Characteristics include management's conservative approach to taking and monitoring business risks; management's moderate attitudes and actions toward financial reporting; and management's attitudes toward information processing, accounting functions, and personnel. Management has formal policies and procedures in place to guide personnel on specific information processing functions. Also, management conducts performance reviews of employees on an annual basis to evaluate performance of employees against expected levels of performance.

Organizational Structure

Management has designed the organizational structure to provide quality service and accountability in support of Luma's mission. To achieve quality in performance, they strive for continuous improvement in what is done, plan and commit to accomplish targets, and are empowered to perform their duties. Policies and communications ensure personnel understand Luma's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Management utilizes organizational charts to communicate key areas of authority, responsibility, and lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Luma's human resource policies and practices are clearly written and communicated where appropriate. Policies and procedures that are listed in the employee handbook include hiring, training, disciplinary actions, and termination procedures. Onboarding and offboarding checklists are used to track their respective procedures. Employees hired complete onboarding requirements prior to the hiring date and thereafter. Onboarding requirements include separate access authorizations, security awareness training, acknowledging the Acceptable Use Policy, criminal background screenings, and signing an agreement stipulating the terms and conditions of employment. Reperformance of training and acknowledgment of the Acceptable Use Policy is required annually thereafter.

Risk Assessment

Risk assessment is the process of identifying and analyzing relevant risks which, if realized, could prevent Luma's management from achieving its operational compliance objectives. Management assesses and manages risks that could affect the organization's ability to provide services to its clients on an ongoing basis. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them.

Objective Setting

The risk assessment process begins by determining the organization's objectives so that associated risks are analyzed and prioritized relative to the achievement of company objectives. A quarterly strategy meeting is held by management to discuss and align the internal control responsibilities, and employee performance measures and incentives with company business objectives. Management has committed to customers to carry out certain objectives in relation to the services provided. These commitments are documented and formally reviewed by management during the risk assessment process to ensure that the operations, reporting, and compliance objectives are aligned with the commitments and company's mission.

Risk Identification and Analysis

Luma's risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Luma's management oversees risk management ownership and accountability and is involved in the risk identification process. Management identifies elements of business risk including threats, vulnerabilities, and safeguards. Identified risks are rated according to their potential impact and the likelihood of occurrence. To supplement the risk assessment process, penetration testing is performed by a third party to identify threats and assess their potential impact to the systems on an annual basis.

The risk analysis process includes the identification of key business processes where potential risk exposures exist, as well as significant changes to those processes. Identified risks are ranked by a product of the impact and probability scores, ranging from one to five, and totaling a maximum risk score of 25. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Assigned risk owners select and develop control activities over technology to mitigate the risks identified during the annual risk assessment process.

Luma's management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the competence and authority. As a result of management's risk assessment, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Risk Factors

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

External Factors

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

Internal Factors

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

Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Risk Mitigation

Risk mitigation activities include the ability to identify, select, and develop corrective actions that sufficiently meet the identified risks. However, the relative costs versus benefits should also be considered when determining the actions to be taken. Corrective action plans are explicitly defined, responsibility assigned to a single point of contact, and tracked in the ticketing system if a system change is required. The organization has documented policies and procedures to guide personnel throughout this process. The risk assessment and mitigation activities also address the risks arising from potential business disruptions. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved annually based on the business impact analysis (BIA) during the annual risk assessment process.

Information and Communication Systems

Information System

Luma's management has documented information security policies and processes to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time sensitive information, and processes for security and system availability purposes that notify key personnel in the event of potential security issues or system outages. Information systems deal not only with internally generated data, but also with information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Pertinent information is communicated in a form and timeframe that enables people to carry out their responsibilities.

Communication System

Management is involved with day-to-day operations and provides personnel with an understanding of their individual roles and responsibilities. The goal of the communication from top management is to ensure personnel understand their own role in the internal control system, as well as how individual activities relate to the work of others. Communication of these responsibilities includes providing necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. Luma's management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed. Additionally, management holds Customer Success team meetings on a monthly basis to discuss and align outreach strategy, expectations, and issue tracking with company business objectives.

Internal Communications

Communication channels are available to employees to enable communication of significant information upstream and downstream. Luma has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for all employees, an instant messaging platform, and the use of email messages to communicate time-sensitive information. On a quarterly basis, the company hosts an offsite all-hands meeting, where they discuss the company's goals and plans. Additionally, an internal collaboration tool is in place to report incidents, concerns, and complaints.

External Communications

Communication channels are also in place to enable effective communication with external parties, such as customers, suppliers, regulators, and shareholders. Luma has implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events, such as new releases and outages. These methods include customer portal dashboard notifications, email messages, system availability status posted on their public website, and multiple customer contact lines to communicate time-sensitive information.

Monitoring

Luma's management performs monitoring activities to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control activities and procedures. Management places emphasis on maintaining sound internal controls, as well as ensuring integrity and ethical values of its employees.

On-Going Monitoring

Luma uses logging and monitoring systems to monitor potential security threats and vulnerabilities as well as system performance and resource utilization. Intrusion detection software is also in place to detect any unusual system activity or access attempts. Users are assigned a unique username, such that individual activities within the system are restricted, logged, and monitored. Potential security violations, including unauthorized attempts to gain access to the system, are periodically reviewed by the information security steering group.

Luma utilizes the following enterprise monitoring tools:

- Amazon CloudWatch – Provides monitoring services for AWS and application resources in real time.
- Amazon GuardDuty – Performs continuous threat detection and analysis services and alerts personnel of potential findings.
- AWS CloudTrail – AWS CloudTrail is a service that allows Luma to continuously monitor and retain account activity related to actions across the AWS management console. It is a service that performs event logging, including authentication.
- AWS Config – Provides continuous monitoring of AWS resource configurations and evaluation of selected configurations against baseline configurations.
- Cloudflare – A web application firewall (WAF) implemented to detect and block attacks on public-facing services, including application resources and application programming interfaces (API).
- Grafana Loki – An enterprise log management and monitoring solution which ingests resource health and event logs from production systems and resources.
- Prometheus – Analyzes log data and alerts personnel with pre-defined thresholds are met.
- Datadog – Enterprise monitoring tool.

Critical Vendor and Sub-Service Organizations Monitoring

Management evaluates the risks associated with the use of a sub-service organizations and vendors during onboarding and has implemented management oversight and monitoring processes to confirm that the organization continues to provide services in a controlled manner. A Third-Party Management Policy is in place that addresses the requirements for a critical vendor or service provider; due diligence process performed prior to vendor onboarding; monitoring of vendors compliance on a periodic basis; and vendor offboarding. Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. Prior to sharing information designated as confidential with third parties, nondisclosure and BAAs, if applicable, are required to be signed. Monitoring procedures are in place to ensure continual compliance by critical vendors and service providers. This includes reviewing audit reports on an annual basis and completion of a privacy and security assessment commensurate with the level of access and risk associated with the service provided.

Evaluating and Communicating Deficiencies

Deficiencies in management's internal control system surface from multiple sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved—who is

in the position to take corrective action, but also to one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and make the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

CATEGORIES, CRITERIA, AND RELATED CONTROLS

The categories, criteria, and related controls are included in Section 4 of this report, “Categories, Criteria, Related Controls and Tests of Operating Effectiveness”, to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the criteria and related controls are included in Section 4, they are, nevertheless, an integral part of the organization’s description of controls.

COMPLEMENTARY CONTROL CONSIDERATIONS

Luma's policies and procedures over its Patient Success Platform Services system cover only a portion of the overall internal control for each user entity. It is not feasible for Luma's service commitments and systems requirements related to the Patient Success Platform Services system to be solely achieved by Luma. Luma's control policies and procedures were designed with the assumption that certain controls would be in place and in operation at the sub-service organizations and user entities. Sub-service organization controls and user entity internal controls must be evaluated, taking into consideration Luma's controls and their own internal controls. Luma's management does not make any representations regarding responsibility related to or provide any assurance regarding any such internal control or regulatory requirements for which the client must assess or comply.

This section describes some of the control considerations for the sub-service organizations and user entities, or "complementary controls", which should be in operation at the sub-service organizations and user entities to complement the controls at the service organization. User auditors / user entities should determine whether the sub-service organizations and user entities have established controls to ensure that the criteria within this report are met. The "complementary controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by the sub-service organizations or user entities.

Complementary User Entity Controls

1. User entities are responsible for administering and monitoring the use of login IDs and passwords provided by Luma for access to the software.
2. User entities are responsible to terminate credentials for personnel whose access is no longer required.

Complementary Sub-Service Organization Controls

1. Sub-service organizations are responsible for implementing control activities to provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.
2. Sub-service organizations are responsible for implementing control activities to provide reasonable assurance that information systems are patched in a timely manner.
3. Sub-service organizations are responsible for implementing environmental control activities to provide reasonable assurance that critical IT infrastructure is protected from certain environmental threats.
4. Sub-service organizations are responsible for notifying Luma of any security-related incidents promptly.
5. Sub-service organizations are responsible for ensuring the ability to read and recover data from physical assets has been diminished prior to the discontinuation of logical and physical protections.

SECTION 4:

CATEGORIES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

INFORMATION PROVIDED BY THE SERVICE AUDITOR

Introduction

This report is intended to provide user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding with information about controls that may affect the Patient Success Platform Services system provided by Luma and to provide information about the operating effectiveness of controls that were tested.

The scope of our testing of Luma's controls was limited to the categories, criteria, and the related controls specified by Luma's management and contained within Section 4 of this report, which management believes to be the relevant key controls for the categories and criteria included in the scope of this report. Our review was not extended to controls in place at any user entities, sub-service organizations, or any other third-party vendors.

The examination was performed in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 21 '*Direct Examination Engagements*', specifically AT-C Section 105, "*Concepts Common to All Attestation Engagements*" and AT-C Section 205, '*Assertion – Based Examination Engagements*.' It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities and the sub-service organizations to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities, the sub-service organizations, and Luma must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "Complementary Control Considerations." If an effectively operating user entity or sub-service organization internal control is not in place, the controls at Luma may not sufficiently compensate for the deficiency.

Tests of Operating Effectiveness

Our tests of the operating effectiveness of the controls specified by Luma's management included such tests as we considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified criteria during the period from May 1, 2024 to April 30, 2025. In selecting particular tests of the operating effectiveness of controls we considered 1) the nature of the controls being tested; 2) the types and completeness of available evidential matter; 3) the nature of the criteria to be achieved; 4) the assessed level of control risk; 5) the expected efficiency and effectiveness of the test; and 6) the testing of other controls relevant to the criteria.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding for the controls specified to achieve the criteria are presented in this section under the column heading "Results of Testing." The concept of materiality is not applied when reporting the results of the tests of controls for which exceptions have been identified because the independent service auditor does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, 360 Advanced, Inc. reports all exceptions. Exceptions identified herein are not necessarily considered significant deficiencies or material weaknesses in the total system of internal controls of Luma, as this determination can only be made after consideration of controls in place at user entities. Control considerations that should be exercised by Luma's clients to complement the controls of Luma to attain the criteria are presented in relation to the nature of services being audited and the controls specified by Luma management.

Types of Tests Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➤ Knowledge and additional information regarding the policy or procedure; and ➤ Corroborating evidence of the policy or procedure.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➤ Examination / Inspection of source documentation and authorizations to verify transactions processed; ➤ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures; ➤ Examination / Inspection of systems documentation, configurations and settings; and ➤ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed

Procedures for Assessing Completeness and Accuracy of IPE

For tests of controls requiring the use of Information Provided by the Entity (“IPE”) (e.g., controls requiring system generated populations for sample-based testing), 360 Advanced, Inc. performed a combination of the following procedures, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, (3) tied data between the IPE and the source, and / or (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintained its integrity. In addition to the above procedures, for tests of controls requiring management’s use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), the independent service auditor inspected management’s procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Sampling Methodology

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2
Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

CATEGORIES, CRITERIA, AND RELATED CONTROLS

Security (Common Criteria to All Categories)

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CTL-001	Management establishes and formally documents entity values and behavioral standards within the company's code of conduct, which is reviewed and updated as needed.	Inquired of the People Operations Generalist to verify that management established and formally documented entity values and behavioral standards within the company's code of conduct, which was reviewed and updated as needed.	No exceptions noted.
		Inspected the Code of Conduct to verify that management established and formally documented entity values and behavioral standards within the company's code of conduct, which was reviewed and updated as needed.	No exceptions noted.
CTL-002	Employees and contractors are required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that employees and contractors were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
		Inspected the signed employment agreements for a sample of employees onboarded during the examination period to verify that employees were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the signed employment agreements for a sample of contractors onboarded during the examination period to verify that contractors were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
CTL-003	An employee sanction clause defining disciplinary action, including termination of employment, for noncompliance with a policy or procedures, are defined and documented.	Inquired of the People Operations Generalist to verify that an employee sanction clause defining disciplinary action, including termination of employment, for noncompliance with a policy or procedures, were defined and documented.	No exceptions noted.
		Inspected the Code of Conduct to verify that an employee sanction clause defining disciplinary action, including termination of employment, for noncompliance with a policy or procedures, were defined and documented.	No exceptions noted.
CTL-012	Annually, management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans.	Inquired of the People Operations Generalist to verify that management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans on an annual basis.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured employees to verify that management performed employee performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured contractors to verify that management performed contractor performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CTL-004	The board of directors establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment.	Inquired of the Director of Information Security and Compliance to verify that the board of directors establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment.	No exceptions noted.
		Inspected the bylaws and board charters to verify that the board of directors establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment.	No exceptions noted.
CTL-005	The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.	Inquired of the Director of Information Security and Compliance to verify that the board of directors has sufficient members who were independent from management and objective in evaluations and decision making.	No exceptions noted.
		Inspected the BOD member listing to verify that the board of directors has sufficient members who were independent from management and objective in evaluations and decision making.	No exceptions noted.
CTL-006	Quarterly, board of directors and committee meetings are held to review internal control performance.	Inquired of the Director of Information Security and Compliance to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
		Inspected the meeting invites and attendees for a sample of quarters during the examination period to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CTL-006	Quarterly, board of directors and committee meetings are held to review internal control performance.	Inquired of the Director of Information Security and Compliance to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
		Inspected the meeting invites and attendees for a sample of quarters during the examination period to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
CTL-007	Organizational charts are in place to communicate the defined key structures, reporting lines, and authorities.	Inquired of the Director of Information Security and Compliance to verify that organizational charts were in place to communicate the defined key structures, reporting lines, and authorities.	No exceptions noted.
		Inspected the organization chart to verify that organizational charts were in place to communicate the defined key structures, reporting lines, and authorities.	No exceptions noted.
CTL-008	Job descriptions defining the competencies and responsibilities required for particular jobs are documented.	Inquired of the People Operations Generalist to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.
		Inspected the IT job descriptions to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.
CTL-009	An information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	Inquired of the Director of Information Security and Compliance to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Roles Policy to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CTL-008	Job descriptions defining the competencies and responsibilities required for particular jobs are documented.	Inquired of the People Operations Generalist to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.
		Inspected the IT job descriptions to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.
CTL-010	Employee hiring procedures are in place to help ensure candidates possess the required skills and technical knowledge to perform the duties as outlined in the job description.	Inquired of the People Operations Generalist to verify that employee hiring procedures were in place to help ensure candidates possessed the required skills and technical knowledge to perform the duties as outlined in the job description.	No exceptions noted.
		Inspected the recruiting workflow and an interview process to verify that employee hiring procedures were in place to help ensure candidates possessed the required skills and technical knowledge to perform the duties as outlined in the job description.	No exceptions noted.
CTL-011	Background screenings are performed on new hire employees as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that background screenings were performed on new hire employees as a component of the onboarding process.	No exceptions noted.
		Inspected the completed background screenings for a sample of employees onboarded during the examination period to verify that background screenings were performed on new hire employees as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-012	Annually, management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans.	Inquired of the People Operations Generalist to verify that management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans on an annual basis.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured employees to verify that management performed employee performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured contractors to verify that management performed contractor performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
CTL-013	Employees and contractors are required to complete security awareness training as a component of the onboarding process.	Inquired of the Information Security Engineer to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
		Inspected the security awareness training records for a sample of employees onboarded during the examination period to verify that contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
		Inspected the security awareness training records for a sample of contractors onboarded during the examination period to verify that contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-014	An employee/contractor checklist is documented to guide personnel in the onboarding of new employees and contractors to ensure that newly hired employees and contractors are compliant with the company's employment standard and corporate policies and procedures.	Inquired of the People Operations Generalist to verify that an employee/contractor checklist was documented to guide personnel in the onboarding of new employees and contractors to ensure that newly hired employees and contractors were compliant with the company's employment standard and corporate policies and procedures.	No exceptions noted.
		Inspected the documented new hire checklist to verify that an employee/contractor checklist was documented to guide personnel in the onboarding of new employees and contractors to ensure that newly hired employees and contractors were compliant with the company's employment standard and corporate policies and procedures.	No exceptions noted.
CTL-024	Annually, employees and contractors are required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inquired of the Information Security Engineer to verify that employees and contractors were required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies on an annual basis.	No exceptions noted.
		Inspected the security awareness training completion records for a sample of tenured employees to verify that employees and contractors were required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies within the past 12 months.	No exceptions noted.
		Inspected the security awareness training completion records for a sample of tenured contractors to verify that contractors were required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CTL-002	Employees and contractors are required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that employees and contractors were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
		Inspected the signed employment agreements for a sample of employees onboarded during the examination period to verify that employees were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
		Inspected the signed employment agreements for a sample of contractors onboarded during the examination period to verify that contractors were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
CTL-004	The board of directors establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment.	Inquired of the Director of Information Security and Compliance to verify that the board of directors establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment.	No exceptions noted.
		Inspected the bylaws and board charters to verify that the board of directors establishes and maintains company bylaws which describe their responsibilities and oversight of management's internal control environment.	No exceptions noted.
CTL-008	Job descriptions defining the competencies and responsibilities required for particular jobs are documented.	Inquired of the People Operations Generalist to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the IT job descriptions to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.
CTL-009	An information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	Inquired of the Director of Information Security and Compliance to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
		Inspected the Roles Policy to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
CTL-012	Annually, management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans.	Inquired of the People Operations Generalist to verify that management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans on an annual basis.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured employees to verify that management performed employee performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured contractors to verify that management performed contractor performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
CTL-015	Monthly, management holds a Customer Success team meeting to discuss and align outreach strategy, expectations, and issue tracking with company business objectives.	Inquired of the Director of Information Security and Compliance to verify that management holds a Customer Success team meeting to discuss and align outreach strategy, expectations, and issue tracking with company business objectives on a monthly basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the meeting invites and attendees from a sample of months during the examination period to verify that management holds a Customer Success team meeting to discuss and align outreach strategy, expectations, and issue tracking with company business objectives on a monthly basis.	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.			
CTL-006	Quarterly, board of directors and committee meetings are held to review internal control performance.	Inquired of the Director of Information Security and Compliance to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
		Inspected the meeting invites and attendees for a sample of quarters during the examination period to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
CTL-016	Documented policies and procedures are in place to identify information required to support the functioning of internal control.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to identify information required to support the functioning of internal control.	No exceptions noted.
		Inspected the company intranet to verify that documented policies and procedures were in place to identify information required to support the functioning of internal control.	No exceptions noted.
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-018	Information security personnel monitor the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	Inquired of the Director of Information Security and Compliance to verify that information security personnel monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
		Inspected the threat subscription emails to verify that information security personnel monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	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.			
CTL-002	Employees and contractors are required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that employees and contractors were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the signed employment agreements for a sample of employees onboarded during the examination period to verify that employees were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
		Inspected the signed employment agreements for a sample of contractors onboarded during the examination period to verify that contractors were required to acknowledge the employment agreement indicating that they understand their responsibilities for adhering to associated policies and procedures as a component of the onboarding process.	No exceptions noted.
CTL-006	Quarterly, board of directors and committee meetings are held to review internal control performance.	Inquired of the Director of Information Security and Compliance to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
		Inspected the meeting invites and attendees for a sample of quarters during the examination period to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
CTL-008	Job descriptions defining the competencies and responsibilities required for particular jobs are documented.	Inquired of the People Operations Generalist to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.
		Inspected the IT job descriptions to verify that job descriptions defining the competencies and responsibilities required for particular jobs were documented.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-009	An information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	Inquired of the Director of Information Security and Compliance to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
		Inspected the Roles Policy to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
CTL-012	Annually, management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans.	Inquired of the People Operations Generalist to verify that management performs employee and contractor performance reviews, covering commitment to company values, training, and development plans on an annual basis.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured employees to verify that management performed employee performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
		Inspected the performance reviews for a sample of tenured contractors to verify that management performed contractor performance reviews, covering commitment to company values, training, and development plans within the past 12 months.	No exceptions noted.
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-020	Quarterly, management meetings are held to discuss internal control responsibilities, company business goals and objectives, and employee performance and incentives.	Inquired of the Director of Information Security and Compliance to verify that management meetings were held to discuss internal control responsibilities, company business goals and objectives, and employee performance and incentives on a quarterly basis.	No exceptions noted.
		Inspected the calendar invites and meeting attendees for a sample of quarters during the examination period to verify that management meetings were held to discuss internal control responsibilities, company business goals and objectives, and employee performance and incentives on a quarterly basis.	No exceptions noted.
CTL-021	Quarterly, all-hands meetings are held to communicate company strategies, goals, and initiatives with employees.	Inquired of the Director of Information Security and Compliance to verify that all-hands meetings were held to communicate company strategies, goals, and initiatives with employees on a quarterly basis.	No exceptions noted.
		Inspected the calendar invites and meeting attendees for a sample of quarters during the examination period to verify that all-hands meetings were held to communicate company strategies, goals, and initiatives with employees on a quarterly basis.	No exceptions noted.
CTL-022	An internal collaboration tool is in place to report incidents, concerns, and complaints.	Inquired of the Director of Information Security and Compliance to verify that an internal collaboration tool was in place to report incidents, concerns, and complaints.	No exceptions noted.
		Inspected the IT support reporting system and incident population to verify that an internal collaboration tool was in place to report incidents, concerns, and complaints.	No exceptions noted.
CTL-023	A confidential communication channel is available to employees for questions or to anonymously report concerns.	Inquired of the People Operations Generalist to verify that a confidential communication channel was available to employees for questions or to anonymously report concerns.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the reporting contact page to verify that a confidential communication channel was available to employees for questions or to anonymously report concerns.	No exceptions noted.
CTL-024	Annually, employees and contractors are required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inquired of the Information Security Engineer to verify that employees and contractors were required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies on an annual basis.	No exceptions noted.
		Inspected the security awareness training completion records for a sample of tenured employees to verify that employees and contractors were required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies within the past 12 months.	No exceptions noted.
		Inspected the security awareness training completion records for a sample of tenured contractors to verify that contractors were required to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies within the past 12 months.	No exceptions noted.
CTL-068	Employees and contractors acknowledge receipt of the Acceptable Use Policy as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that employees and contractors acknowledged receipt of the Acceptable Use Policy as a component of the onboarding process.	No exceptions noted.
		Inspected the policy acknowledgement records for a sample of employees onboarded during the examination period to verify that employees acknowledged receipt of the Acceptable Use Policy as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the policy acknowledgement records for a sample of contractors onboarded during the examination period to verify that contractors acknowledged receipt of the Acceptable Use Policy as a component of the onboarding process.	No exceptions noted.
CTL-073	Annually, employees and contractors acknowledge the Acceptable Use Policy to confirm their commitment towards information security.	Inquired of the Director of Information Security and Compliance to verify that employees and contractors acknowledge the Acceptable Use Policy to confirm their commitment towards information security on an annual basis.	No exceptions noted.
		Inspected the Acceptable Use Policy acknowledgement records for a sample of tenured employees during the examination period to verify that employees acknowledged the Acceptable Use Policy to confirm their commitment towards information security within the past 12 months.	No exceptions noted.
		Inspected the Acceptable Use Policy acknowledgement records for a sample of tenured contractors during the examination period to verify that contractors acknowledged the Acceptable Use Policy to confirm their commitment towards information security within the past 12 months.	No exceptions noted.
CTL-074	An incident response plan is maintained by management to guide employees in identifying and elevating security incidents.	Inquired of the Director of Information Security and Compliance to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
		Inspected the Incident Response Policy and planning documents to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
CTL-077	A ticketing system is used to track identified incidents through remediation.	Inquired of the Director of Information Security and Compliance to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the incident tickets for a sample of incidents that occurred during the examination period to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CTL-025	The entity's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements, are documented in customer contracts and nondisclosure agreements.	Inquired of the People Operations Generalist to verify that the entity's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements, were documented in customer contracts and nondisclosure agreements.	No exceptions noted.
		Inspected the agreements executed with a sample of customers onboarded during the examination period to verify that the entity's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements, were documented in customer contracts and nondisclosure agreements.	No exceptions noted.
CTL-026	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.	Inquired of the Director of Information Security and Compliance to verify that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.
		Inspected the company website resources to verify that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.
CTL-027	Incident and escalation reporting procedures are in place for customers to report system failures, incidents, and complaints. Reports of concerns are reviewed by the customer success team on an as needed basis.	Inquired of the Director of Information Security and Compliance to verify that incident and escalation reporting procedures were in place for customers to report system failures, incidents, and complaints. Reports of concerns were reviewed by the customer success team on an as needed basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the company website and application dashboard and the support and issue tracking system to verify that incident and escalation reporting procedures were in place for customers to report system failures, incidents, and complaints. Reports of concerns were reviewed by the customer success team on an as needed basis.	No exceptions noted.
CTL-028	Releases and outages affecting system availability are communicated to customers through monthly newsletters and customer dashboards.	Inquired of the Director of Information Security and Compliance to verify that releases and outages affecting system availability were communicated to customers through monthly newsletters and customer dashboards.	No exceptions noted.
		Inspected the monthly newsletter and the system status page to verify that releases and outages affecting system availability were communicated to customers through monthly newsletters and customer dashboards.	No exceptions noted.
CTL-067	A signed BAA for confidentiality and protection is executed with critical vendors and service providers as a component of the onboarding process.	Inquired of the Director of Information Security and Compliance to verify that a signed BAA for confidentiality and protection was executed with critical vendors and service providers as a component of the onboarding process.	No exceptions noted.
		Inspected the executed BAA for the population of vendors onboarded within the examination period to verify that a signed BAA for confidentiality and protection was executed with critical vendors and service providers as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-009	An information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	Inquired of the Director of Information Security and Compliance to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
		Inspected the Roles Policy to verify that an information security management team has been established to maintain and enforce security policies and procedures throughout the organization.	No exceptions noted.
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-029	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
		Inspected the Risk Management Policy and vulnerability scanning policy to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-075	Annually, a BIA is performed by management.	Inquired of the Director of Information Security and Compliance to verify that a BIA was performed by management on an annual basis.	No exceptions noted.
		Inspected the most recent BIA to verify that a BIA was performed by management within the past 12 months.	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.			
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-029	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
		Inspected the Risk Management Policy and vulnerability scanning policy to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
CTL-031	Annually, penetration testing is performed by a third party to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems on an annual basis.	No exceptions noted.
		Inspected the most recent penetration test report to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems within the past 12 months.	No exceptions noted.
CTL-032	Results of external audits are included in the risk assessment and remediations are monitored through resolution.	Inquired of the Director of Information Security and Compliance to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
		Inspected the penetration testing report, the risk register and a meeting invite to review a third party issued compliance report to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
CTL-033	Monthly, an enterprise security tool is utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the vulnerability assessment results for a sample of months during the examination period to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CTL-011	Background screenings are performed on new hire employees as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that background screenings were performed on new hire employees as a component of the onboarding process.	No exceptions noted.
		Inspected the completed background screenings for a sample of employees onboarded during the examination period to verify that background screenings were performed on new hire employees as a component of the onboarding process.	No exceptions noted.
CTL-023	A confidential communication channel is available to employees for questions or to anonymously report concerns.	Inquired of the People Operations Generalist to verify that a confidential communication channel was available to employees for questions or to anonymously report concerns.	No exceptions noted.
		Inspected the reporting contact page to verify that a confidential communication channel was available to employees for questions or to anonymously report concerns.	No exceptions noted.
CTL-034	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.
		Inspected the Risk Management Policy to verify that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-035	Annually, management performs a risk assessment that considers the potential for fraud.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that considers the potential for fraud on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment within the past 12 months that considers the potential for fraud.	No exceptions noted.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-018	Information security personnel monitor the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	Inquired of the Director of Information Security and Compliance to verify that information security personnel monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
		Inspected the threat subscription emails to verify that information security personnel monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
CTL-029	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Risk Management Policy and vulnerability scanning policy to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	No exceptions noted.
CTL-057	Application development and change management procedures are documented to guide personnel in the SDLC and change management process.	Inquired of the Director of Information Security and Compliance to verify that application development and change management procedures were documented to guide personnel in the SDLC and change management process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Configuration Management Policy to verify that application development and change management procedures were documented to guide personnel in the SDLC and change management process.	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.			
CTL-006	Quarterly, board of directors and committee meetings are held to review internal control performance.	Inquired of the Director of Information Security and Compliance to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
		Inspected the meeting invites and attendees for a sample of quarters during the examination period to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
CTL-031	Annually, penetration testing is performed by a third party to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems on an annual basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the most recent penetration test report to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems within the past 12 months.	No exceptions noted.
CTL-032	Results of external audits are included in the risk assessment and remediations are monitored through resolution.	Inquired of the Director of Information Security and Compliance to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
		Inspected the penetration testing report, the risk register and a meeting invite to review a third party issued compliance report to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
CTL-033	Monthly, an enterprise security tool is utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
		Inspected the vulnerability assessment results for a sample of months during the examination period to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
CTL-036	Documented policies and procedures are in place to guide personnel in defining the audit scope and performing the internal system audit process.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in defining the audit scope and performing the internal system audit process.	No exceptions noted.
		Inspected the Auditing Policy to verify that documented policies and procedures were in place to guide personnel in defining the audit scope and performing the internal system audit process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-006	Quarterly, board of directors and committee meetings are held to review internal control performance.	Inquired of the Director of Information Security and Compliance to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
		Inspected the meeting invites and attendees for a sample of quarters during the examination period to verify that board of directors and committee meetings were held to review internal control performance on a quarterly basis.	No exceptions noted.
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
CTL-031	Annually, penetration testing is performed by a third party to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems on an annual basis.	No exceptions noted.
		Inspected the most recent penetration test report to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-032	Results of external audits are included in the risk assessment and remediations are monitored through resolution.	Inquired of the Director of Information Security and Compliance to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
		Inspected the penetration testing report, the risk register and a meeting invite to review a third party issued compliance report to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
CTL-033	Monthly, an enterprise security tool is utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
		Inspected the vulnerability assessment results for a sample of months during the examination period to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
CTL-074	An incident response plan is maintained by management to guide employees in identifying and elevating security incidents.	Inquired of the Director of Information Security and Compliance to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
		Inspected the Incident Response Policy and planning documents to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-029	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
		Inspected the Risk Management Policy and vulnerability scanning policy to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	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.			
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-029	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
		Inspected the Risk Management Policy and vulnerability scanning policy to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
CTL-037	Assigned risk owners select and develop control activities over technology to mitigate the risks identified during the annual risk assessment process.	Inquired of the Director of Information Security and Compliance to verify that assigned risk owners select and develop control activities over technology to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.
		Inspected the security risk register to verify that assigned risk owners select and develop control activities over technology to mitigate the risks identified during the annual risk assessment process.	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.			
CTL-003	An employee sanction clause defining disciplinary action, including termination of employment, for noncompliance with a policy or procedures, are defined and documented.	Inquired of the People Operations Generalist to verify that an employee sanction clause defining disciplinary action, including termination of employment, for noncompliance with a policy or procedures, were defined and documented.	No exceptions noted.
		Inspected the Code of Conduct to verify that an employee sanction clause defining disciplinary action, including termination of employment, for noncompliance with a policy or procedures, were defined and documented.	No exceptions noted.
CTL-016	Documented policies and procedures are in place to identify information required to support the functioning of internal control.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to identify information required to support the functioning of internal control.	No exceptions noted.
		Inspected the company intranet to verify that documented policies and procedures were in place to identify information required to support the functioning of internal control.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-050	Customer data is disposed according to the Luma data retention policy.	Inquired of the Director of Information Security and Compliance to verify that customer data was disposed according to the Luma data retention policy.	No exceptions noted.
		Inspected the Data Retention Policy and the data deletion records for a sample of customers offboarded during the examination period to verify that customer data was disposed according to the Luma data retention policy.	No exceptions noted.
CTL-057	Application development and change management procedures are documented to guide personnel in the SDLC and change management process.	Inquired of the Director of Information Security and Compliance to verify that application development and change management procedures were documented to guide personnel in the SDLC and change management process.	No exceptions noted.
		Inspected the Configuration Management Policy to verify that application development and change management procedures were documented to guide personnel in the SDLC and change management process.	No exceptions noted.
CTL-065	A documented third party management policy is in place to ensure the coordinated and consistent management of third parties.	Inquired of the Director of Information Security and Compliance to verify that a documented third party management policy was in place to ensure the coordinated and consistent management of third parties.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Third Party Policy to verify that a documented third party management policy was in place to ensure the coordinated and consistent management of third parties.	No exceptions noted.
CTL-068	Employees and contractors acknowledge receipt of the Acceptable Use Policy as a component of the onboarding process.	Inquired of the People Operations Generalist to verify that employees and contractors acknowledged receipt of the Acceptable Use Policy as a component of the onboarding process.	No exceptions noted.
		Inspected the policy acknowledgement records for a sample of employees onboarded during the examination period to verify that employees acknowledged receipt of the Acceptable Use Policy as a component of the onboarding process.	No exceptions noted.
		Inspected the policy acknowledgement records for a sample of contractors onboarded during the examination period to verify that contractors acknowledged receipt of the Acceptable Use Policy as a component of the onboarding process.	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.			
CTL-038	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.
		Inspected the Human Resources Security and System Access policies to verify that documented policies and procedures were in place to guide personnel regarding access provisioning, modification, removal, and review.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-039	User access requests are documented and approved by management prior to provisioning access to in-scope systems.	Inquired of the Director of Information Security and Compliance to verify that user access requests were documented and approved by management prior to provisioning access to in-scope systems.	No exceptions noted.
		Inspected the user access requests for a sample of employees and contractors onboarded during the examination period to verify that user access requests were documented and approved by management prior to provisioning access to in-scope systems.	No exceptions noted.
CTL-040	The in-scope systems are configured to authenticate users with unique user credentials and enforce minimum password requirements and/or multi-factor authentication.	Inquired of the Director of Information Security and Compliance to verify that the in-scope systems were configured to authenticate users with unique user credentials and enforce minimum password requirements and/or multi-factor authentication.	No exceptions noted.
		Inspected the user listings and password configurations for in-scope systems to verify that the in-scope systems were configured to authenticate users with unique user credentials and enforce minimum password requirements and/or multi-factor authentication.	No exceptions noted.
CTL-041	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inquired of the Director of Information Security and Compliance to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
		Inspected the system user listings and predefined user access permission sets to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
CTL-042	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inquired of the Director of Information Security and Compliance to verify that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the product and role permissions matrix, administrator user listings, and employee roster to verify that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CTL-043	An enterprise log management solution is utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviews the alerts and performs remediation activities on an ad-hoc basis.	Inquired of the Director of Information Security and Compliance to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.
		Inspected the alert configurations, an example alert, and the log dashboard to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.
CTL-044	AWS Security Groups are in place and configured to filter unauthorized inbound network traffic from external sources.	Inquired of the Director of Information Security and Compliance to verify that AWS Security Groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
		Inspected the AWS security groups ruleset to verify that AWS security groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
CTL-045	Web sessions are encrypted using TLS encryption protocol.	Inquired of the Director of Information Security and Compliance to verify that web sessions were encrypted using TLS encryption protocol.	No exceptions noted.
		Inspected the encryption configurations to verify that web sessions were encrypted using TLS encryption protocol.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-046	An encrypted VPN is utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	Inquired of the Director of Information Security and Compliance to verify that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	No exceptions noted.
		Inspected the VPN configurations to verify that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	No exceptions noted.
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	No exceptions noted.
CTL-078	The MDM platform provides the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	Inquired of the Director of Information Security and Compliance to verify that the MDM platform provided the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	No exceptions noted.
		Inspected the remote wipe configurations and an example event log to verify that the MDM platform provided the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
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.			
CTL-039	User access requests are documented and approved by management prior to provisioning access to in-scope systems.	Inquired of the Director of Information Security and Compliance to verify that user access requests were documented and approved by management prior to provisioning access to in-scope systems.	No exceptions noted.
		Inspected the user access requests for a sample of employees and contractors onboarded during the examination period to verify that user access requests were documented and approved by management prior to provisioning access to in-scope systems.	No exceptions noted.
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	No exceptions noted.
CTL-048	IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process.	Inquired of the Director of Information Security and Compliance to verify that IT personnel revoked terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the active user listing and access revocation records for a sample of employees and contractors offboarded during the examination period to verify that IT personnel revoked terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.
CTL-049	Semi-annually, a user access review is performed to help ensure that access to in-scope systems are restricted.	Inquired of the Director of Information Security and Compliance to verify that a user access review was performed on a semi-annual basis to help ensure that access to in-scope systems were restricted.	No exceptions noted.
		Inspected the completed access reviews for the in-scope systems to verify that a user access review was performed on a semi-annual basis to help ensure that access to in-scope systems were restricted.	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.			
CTL-039	User access requests are documented and approved by management prior to provisioning access to in-scope systems.	Inquired of the Director of Information Security and Compliance to verify that user access requests were documented and approved by management prior to provisioning access to in-scope systems.	No exceptions noted.
		Inspected the user access requests for a sample of employees and contractors onboarded during the examination period to verify that user access requests were documented and approved by management prior to provisioning access to in-scope systems.	No exceptions noted.
CTL-040	The in-scope systems are configured to authenticate users with unique user credentials and enforce minimum password requirements and/or multi-factor authentication.	Inquired of the Director of Information Security and Compliance to verify that the in-scope systems were configured to authenticate users with unique user credentials and enforce minimum password requirements and/or multi-factor authentication.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the user listings and password configurations for in-scope systems to verify that the in-scope systems were configured to authenticate users with unique user credentials and enforce minimum password requirements and/or multi-factor authentication.	No exceptions noted.
CTL-041	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inquired of the Director of Information Security and Compliance to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
		Inspected the system user listings and predefined user access permission sets to verify that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
CTL-042	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inquired of the Director of Information Security and Compliance to verify that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the product and role permissions matrix, administrator user listings, and employee roster to verify that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CTL-048	IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process.	Inquired of the Director of Information Security and Compliance to verify that IT personnel revoked terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.
		Inspected the active user listing and access revocation records for a sample of employees and contractors offboarded during the examination period to verify that IT personnel revoked terminated employees' access to the in-scope systems as a component of the termination process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-049	Semi-annually, a user access review is performed to help ensure that access to in-scope systems are restricted.	Inquired of the Director of Information Security and Compliance to verify that a user access review was performed on a semi-annual basis to help ensure that access to in-scope systems were restricted.	No exceptions noted.
		Inspected the completed access reviews for the in-scope systems to verify that a user access review was performed on a semi-annual basis to help ensure that access to in-scope systems were restricted.	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.			
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	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.			
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	No exceptions noted.
CTL-050	Customer data is disposed according to the Luma data retention policy.	Inquired of the Director of Information Security and Compliance to verify that customer data was disposed according to the Luma data retention policy.	No exceptions noted.
		Inspected the Data Retention Policy and the data deletion records for a sample of customers offboarded during the examination period to verify that customer data was disposed according to the Luma data retention policy.	No exceptions noted.
CTL-078	The MDM platform provides the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	Inquired of the Director of Information Security and Compliance to verify that the MDM platform provided the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	No exceptions noted.
		Inspected the remote wipe configurations and an example event log to verify that the MDM platform provided the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CTL-043	An enterprise log management solution is utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviews the alerts and performs remediation activities on an ad-hoc basis.	Inquired of the Director of Information Security and Compliance to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the alert configurations, an example alert, and the log dashboard to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.
CTL-044	AWS Security Groups are in place and configured to filter unauthorized inbound network traffic from external sources.	Inquired of the Director of Information Security and Compliance to verify that AWS Security Groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
		Inspected the AWS security groups ruleset to verify that AWS security groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
CTL-045	Web sessions are encrypted using TLS encryption protocol.	Inquired of the Director of Information Security and Compliance to verify that web sessions were encrypted using TLS encryption protocol.	No exceptions noted.
		Inspected the encryption configurations to verify that web sessions were encrypted using TLS encryption protocol.	No exceptions noted.
CTL-046	An encrypted VPN is utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	Inquired of the Director of Information Security and Compliance to verify that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	No exceptions noted.
		Inspected the VPN configurations to verify that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	No exceptions noted.
CTL-051	A monitoring tool is in place to monitor the performance and availability of website services and to help identify potential sources of failure.	Inquired of the Director of Information Security and Compliance to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
		Inspected the monitoring tool dashboard and alert configurations to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
CTL-052	Monitoring tools are in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	Inquired of the Director of Information Security and Compliance to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
		Inspected the configuration for monitoring tools and example alerts to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-056	A WAF is utilized to monitor and analyze web application events for possible or actual security breaches.	Inquired of the Director of Information Security and Compliance to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	No exceptions noted.
		Inspected the WAF configurations and rulesets to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	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.			
CTL-044	AWS Security Groups are in place and configured to filter unauthorized inbound network traffic from external sources.	Inquired of the Director of Information Security and Compliance to verify that AWS Security Groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
		Inspected the AWS security groups ruleset to verify that AWS security groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
CTL-045	Web sessions are encrypted using TLS encryption protocol.	Inquired of the Director of Information Security and Compliance to verify that web sessions were encrypted using TLS encryption protocol.	No exceptions noted.
		Inspected the encryption configurations to verify that web sessions were encrypted using TLS encryption protocol.	No exceptions noted.
CTL-046	An encrypted VPN is utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	Inquired of the Director of Information Security and Compliance to verify that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	No exceptions noted.
		Inspected the VPN configurations to verify that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-053	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths.	Inquired of the Director of Information Security and Compliance to verify that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths.	No exceptions noted.
		Inspected the Data Integrity Policy to verify that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths.	No exceptions noted.
CTL-054	Customer data is stored in an encrypted format.	Inquired of the Director of Information Security and Compliance to verify that customer data was stored in an encrypted format.	No exceptions noted.
		Inspected the production database configurations to verify that customer data was stored in an encrypted format.	No exceptions noted.
CTL-078	The MDM platform provides the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	Inquired of the Director of Information Security and Compliance to verify that the MDM platform provided the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	No exceptions noted.
		Inspected the remote wipe configurations and an example event log to verify that the MDM platform provided the capability to remotely wipe devices in the event of loss, theft, or upon user termination.	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.			
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-044	AWS Security Groups are in place and configured to filter unauthorized inbound network traffic from external sources.	Inquired of the Director of Information Security and Compliance to verify that AWS Security Groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
		Inspected the AWS security groups ruleset to verify that AWS security groups were in place and configured to filter unauthorized inbound network traffic from external sources.	No exceptions noted.
CTL-055	Antivirus software is configured on workstations and mobile devices for real-time protection against malware.	Inquired of the Director of Information Security and Compliance to verify that antivirus software was configured on workstations and mobile devices for real-time protection against malware.	No exceptions noted.
		Inspected the antivirus software dashboard and configurations to verify that antivirus software was configured on workstations and mobile devices for real-time protection against malware.	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.			
CTL-031	Annually, penetration testing is performed by a third party to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems on an annual basis.	No exceptions noted.
		Inspected the most recent penetration test report to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-032	Results of external audits are included in the risk assessment and remediations are monitored through resolution.	Inquired of the Director of Information Security and Compliance to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
		Inspected the penetration testing report, the risk register and a meeting invite to review a third party issued compliance report to verify that results of external audits were included in the risk assessment and remediations were monitored through resolution.	No exceptions noted.
CTL-033	Monthly, an enterprise security tool is utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
		Inspected the vulnerability assessment results for a sample of months during the examination period to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
CTL-051	A monitoring tool is in place to monitor the performance and availability of website services and to help identify potential sources of failure.	Inquired of the Director of Information Security and Compliance to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
		Inspected the monitoring tool dashboard and alert configurations to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
CTL-052	Monitoring tools are in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	Inquired of the Director of Information Security and Compliance to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the configuration for monitoring tools and example alerts to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
CTL-056	A WAF is utilized to monitor and analyze web application events for possible or actual security breaches.	Inquired of the Director of Information Security and Compliance to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	No exceptions noted.
		Inspected the WAF configurations and rulesets to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	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.			
CTL-031	Annually, penetration testing is performed by a third party to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems on an annual basis.	No exceptions noted.
		Inspected the most recent penetration test report to verify that penetration testing was performed by a third party to identify threats and assess their potential impact to the systems within the past 12 months.	No exceptions noted.
CTL-033	Monthly, an enterprise security tool is utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems.	Inquired of the Director of Information Security and Compliance to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the vulnerability assessment results for a sample of months during the examination period to verify that an enterprise security tool was utilized to perform vulnerability assessments to identify threats and assess their potential impact to the systems on a monthly basis.	No exceptions noted.
CTL-043	An enterprise log management solution is utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviews the alerts and performs remediation activities on an ad-hoc basis.	Inquired of the Director of Information Security and Compliance to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.
		Inspected the alert configurations, an example alert, and the log dashboard to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.
CTL-051	A monitoring tool is in place to monitor the performance and availability of website services and to help identify potential sources of failure.	Inquired of the Director of Information Security and Compliance to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
		Inspected the monitoring tool dashboard and alert configurations to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
CTL-052	Monitoring tools are in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	Inquired of the Director of Information Security and Compliance to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the configuration for monitoring tools and example alerts to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
CTL-056	A WAF is utilized to monitor and analyze web application events for possible or actual security breaches.	Inquired of the Director of Information Security and Compliance to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	No exceptions noted.
		Inspected the WAF configurations and rulesets to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	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.			
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-043	An enterprise log management solution is utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviews the alerts and performs remediation activities on an ad-hoc basis.	Inquired of the Director of Information Security and Compliance to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the alert configurations, an example alert, and the log dashboard to verify that an enterprise log management solution was utilized to provide centralized log storage, event correlation, and alerting of security events on critical systems. Management reviewed the alerts and performed remediation activities on an ad-hoc basis.	No exceptions noted.
CTL-051	A monitoring tool is in place to monitor the performance and availability of website services and to help identify potential sources of failure.	Inquired of the Director of Information Security and Compliance to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
		Inspected the monitoring tool dashboard and alert configurations to verify that a monitoring tool was in place to monitor the performance and availability of website services and to help identify potential sources of failure.	No exceptions noted.
CTL-052	Monitoring tools are in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	Inquired of the Director of Information Security and Compliance to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
		Inspected the configuration for monitoring tools and example alerts to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
CTL-056	A WAF is utilized to monitor and analyze web application events for possible or actual security breaches.	Inquired of the Director of Information Security and Compliance to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	No exceptions noted.
		Inspected the WAF configurations and rulesets to verify that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-074	An incident response plan is maintained by management to guide employees in identifying and elevating security incidents.	Inquired of the Director of Information Security and Compliance to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
		Inspected the Incident Response Policy and planning documents to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
CTL-076	Annually, incident response training and testing is performed to communicate incident response and handling procedures to personnel with incident management roles.	Inquired of the Director of Information Security and Compliance to verify that incident response training and testing was performed on an annual basis to communicate incident response and handling procedures to personnel with incident management roles.	No exceptions noted.
		Inspected the incident management & disaster recovery failover test results to verify that incident response training and testing was performed within the past 12 months to communicate incident response and handling procedures to personnel with incident management roles.	No exceptions noted.
CTL-077	A ticketing system is used to track identified incidents through remediation.	Inquired of the Director of Information Security and Compliance to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.
		Inspected the incident tickets for a sample of incidents that occurred during the examination period to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.
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.			
CTL-013	Employees and contractors are required to complete security awareness training as a component of the onboarding process.	Inquired of the Information Security Engineer to verify that employees and contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the security awareness training records for a sample of employees onboarded during the examination period to verify that contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
		Inspected the security awareness training records for a sample of contractors onboarded during the examination period to verify that contractors were required to complete security awareness training as a component of the onboarding process.	No exceptions noted.
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-074	An incident response plan is maintained by management to guide employees in identifying and elevating security incidents.	Inquired of the Director of Information Security and Compliance to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
		Inspected the Incident Response Policy and planning documents to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
CTL-076	Annually, incident response training and testing is performed to communicate incident response and handling procedures to personnel with incident management roles.	Inquired of the Director of Information Security and Compliance to verify that incident response training and testing was performed on an annual basis to communicate incident response and handling procedures to personnel with incident management roles.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the incident management & disaster recovery failover test results to verify that incident response training and testing was performed within the past 12 months to communicate incident response and handling procedures to personnel with incident management roles.	No exceptions noted.
CTL-077	A ticketing system is used to track identified incidents through remediation.	Inquired of the Director of Information Security and Compliance to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.
		Inspected the incident tickets for a sample of incidents that occurred during the examination period to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CTL-019	Incident response policy and procedures are in place to guide employees in reporting system failures, incidents, and complaints.	Inquired of the Director of Information Security and Compliance to verify that incident response policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
		Inspected the Incident Response Policy to verify that Incident Response Policy and procedures were in place to guide employees in reporting system failures, incidents, and complaints.	No exceptions noted.
CTL-074	An incident response plan is maintained by management to guide employees in identifying and elevating security incidents.	Inquired of the Director of Information Security and Compliance to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
		Inspected the Incident Response Policy and planning documents to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-077	A ticketing system is used to track identified incidents through remediation.	Inquired of the Director of Information Security and Compliance to verify that a ticketing system was used to track identified incidents through remediation.	No exceptions noted.
		Inspected the incident tickets for a sample of incidents that occurred during the examination period to verify that a ticketing system was used to track identified incidents through remediation.	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.			
CTL-052	Monitoring tools are in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	Inquired of the Director of Information Security and Compliance to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
		Inspected the configuration for monitoring tools and example alerts to verify that monitoring tools were in place to detect potential unauthorized changes to in-scope systems. Management reviews the alerts and performs remediation activities as necessary.	No exceptions noted.
CTL-057	Application development and change management procedures are documented to guide personnel in the SDLC and change management process.	Inquired of the Director of Information Security and Compliance to verify that application development and change management procedures were documented to guide personnel in the SDLC and change management process.	No exceptions noted.
		Inspected the Configuration Management Policy to verify that application development and change management procedures were documented to guide personnel in the SDLC and change management process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-058	An automated ticketing system is in place to centrally maintain, manage, and monitor application and infrastructure changes from development through implementation.	Inquired of the Director of Information Security and Compliance to verify that an automated ticketing system was in place to centrally maintain, manage, and monitor application and infrastructure changes from development through implementation.	No exceptions noted.
		Inspected the change records and source code repository to verify that an automated ticketing system was in place to centrally maintain, manage, and monitor application and infrastructure changes from development through implementation.	No exceptions noted.
CTL-059	A version control software allows for rollback of changes when changes impair system operation.	Inquired of the Director of Information Security and Compliance to verify that a version control software allowed for rollback of changes when changes impaired system operation.	No exceptions noted.
		Inspected the branch version listing and a branch rollback configuration to verify that a version control software allowed for rollback of changes when changes impaired system operation.	No exceptions noted.
CTL-060	Development, QA, and production environments are logically segmented.	Inquired of the Director of Information Security and Compliance to verify that development, QA, and production environments were logically segmented.	No exceptions noted.
		Inspected the AWS environment listing to verify that development, QA, and production environments were logically segmented.	No exceptions noted.
CTL-061	The ability to implement changes to the production environment is restricted to personnel commensurate with their job role.	Inquired of the Information Security Engineer to verify that the ability to implement changes to the production environment was restricted to personnel commensurate with their job role.	No exceptions noted.
		Inspected the deployment tool user listing and access logs to verify that the ability to implement changes to the production environment was restricted to personnel commensurate with their job role.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-069	Infrastructure changes are peer reviewed for appropriateness of code change and secure coding techniques prior to implementation in the production environment.	Inquired of the Director of Information Security and Compliance to verify that infrastructure changes were peer reviewed for appropriateness of code change and secure coding techniques prior to implementation in the production environment.	No exceptions noted.
		Inspected the code reviews for a sample of infrastructure changes deployed to the production environment during the examination period to verify that infrastructure changes were peer reviewed for appropriateness of code change and secure coding techniques prior to implementation in the production environment.	No exceptions noted.
CTL-070	Infrastructure changes are approved by management prior to migration to the production environment.	Inquired of the Director of Information Security and Compliance to verify that infrastructure changes were approved by management prior to migration to the production environment.	No exceptions noted.
		Inspected the manager approval records for a sample of infrastructure changes deployed to the production environment during the examination period to verify that infrastructure changes were approved by management prior to migration to the production environment.	No exceptions noted.
CTL-071	Application changes are tested and reviewed by QA personnel prior to releasing to the production environment.	Inquired of the Director of Information Security and Compliance to verify that application changes were tested and reviewed by QA personnel prior to releasing to the production environment.	No exceptions noted.
		Inspected the QA records for a sample of application changes deployed to the production environment during the examination period to verify that application changes were tested and reviewed by QA personnel prior to releasing to the production environment.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-072	Changes to the application are approved by management prior to migration to the production environment.	Inquired of the Director of Information Security and Compliance to verify that changes to the application were approved by management prior to migration to the production environment.	No exceptions noted.
		Inspected the manager approval records for a sample of application changes deployed to the production environment during the examination period to verify that changes to the application were approved by management prior to migration to the production environment.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CTL-017	Annually, management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives.	Inquired of the Director of Information Security and Compliance to verify that management performs a risk assessment that includes identification and assessment of risks for achieving information security objectives on an annual basis.	No exceptions noted.
		Inspected the most recent risk assessment to verify that management performed a risk assessment that included identification and assessment of risks for achieving information security objectives within the past 12 months.	No exceptions noted.
CTL-029	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	Inquired of the Director of Information Security and Compliance to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Risk Management Policy and vulnerability scanning policy to verify that documented policies and procedures were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security of data and service.	No exceptions noted.
CTL-030	Risks identified during the annual risk assessment and security assessments are rated using a risk evaluation process and are documented and tracked to resolution.	Inquired of the Director of Information Security and Compliance to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
		Inspected the security risk register to verify that risks identified during the annual risk assessment and security assessments were rated using a risk evaluation process and were documented and tracked to resolution.	No exceptions noted.
CTL-063	A disaster recovery and business continuity plan are in place to guide personnel in procedures to minimize disruptions to the business caused by an unexpected event.	Inquired of the Director of Information Security and Compliance to verify that a disaster recovery and business continuity plan were in place to guide personnel in procedures to minimize disruptions to the business caused by an unexpected event.	No exceptions noted.
		Inspected the Disaster Recovery Policy to verify that a disaster recovery and business continuity plan were in place to guide personnel in procedures to minimize disruptions to the business caused by an unexpected event.	No exceptions noted.
CTL-064	Annually, a disaster recovery plan exercise is performed to test the disaster recovery plan.	Inquired of the Director of Information Security and Compliance to verify that a disaster recovery plan exercise was performed to test the disaster recovery plan on an annual basis.	No exceptions noted.
		Inspected the most recent disaster recovery exercise report to verify that a disaster recovery plan exercise was performed to test the disaster recovery plan within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-074	An incident response plan is maintained by management to guide employees in identifying and elevating security incidents.	Inquired of the Director of Information Security and Compliance to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
		Inspected the Incident Response Policy and planning documents to verify that an incident response plan was maintained by management to guide employees in identifying and elevating security incidents.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CTL-047	Annually, the compliance team reviews service provider audit reports to ensure that critical vendors and service providers are in compliance with the organization's security commitments.	Inquired of the Director of Information Security and Compliance to verify that the compliance team reviews service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments on an annual basis.	No exceptions noted.
		Inspected the audit reports and vendor review support for a sample of critical vendors and service providers to verify that the compliance team reviewed service provider audit reports to ensure that critical vendors and service providers were in compliance with the organization's security commitments within the past 12 months.	No exceptions noted.
CTL-065	A documented third party management policy is in place to ensure the coordinated and consistent management of third parties.	Inquired of the Director of Information Security and Compliance to verify that a documented third party management policy was in place to ensure the coordinated and consistent management of third parties.	No exceptions noted.
		Inspected the Third Party Policy to verify that a documented third party management policy was in place to ensure the coordinated and consistent management of third parties.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CTL-066	Management performs due diligence on its critical vendors and service providers to ensure third parties are in compliance with the organization's security commitments as a component of the onboarding process.	Inquired of the Director of Information Security and Compliance to verify that management performs due diligence on its critical vendors and service providers to ensure third parties were in compliance with the organization's security commitments as a component of the onboarding process.	No exceptions noted.
		Inspected the pre-vetting and due diligence records for the population of service providers onboarded during the examination period to verify that management performs due diligence on its critical vendors and service providers to ensure third parties were in compliance with the organization's security commitments as a component of the onboarding process.	No exceptions noted.
CTL-067	A signed BAA for confidentiality and protection is executed with critical vendors and service providers as a component of the onboarding process.	Inquired of the Director of Information Security and Compliance to verify that a signed BAA for confidentiality and protection was executed with critical vendors and service providers as a component of the onboarding process.	No exceptions noted.
		Inspected the executed BAA for the population of vendors onboarded within the examination period to verify that a signed BAA for confidentiality and protection was executed with critical vendors and service providers as a component of the onboarding process.	No exceptions noted.