A-LIGN

A-LIGN.com

# Type 2 SOC 2

Prepared for:
Yanka Industries Inc. dba
MasterClass

Year:
2025



# REPORT ON YANKA INDUSTRIES INC. DBA MASTERCLASS' DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

**Pursuant to Reporting on System and Organization Controls 2 (SOC 2)**
**Type 2 examination performed under AT-C 105 and AT-C 205**

**January 1, 2025 to December 31, 2025**

## Table of Contents

**SECTION 1 ASSERTION OF YANKA INDUSTRIES INC. DBA MASTERCLASS MANAGEMENT ..... 1**

**SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT ..... 3**

**SECTION 3 YANKA INDUSTRIES INC. DBA MASTERCLASS' DESCRIPTION OF ITS MASTERCLASS SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2025 TO DECEMBER 31, 2025 ..... 7**

OVERVIEW OF OPERATIONS ..... 8
Company Background ..... 8
Description of Services Provided ..... 8
Principal Service Commitments and System Requirements ..... 8
Components of the System ..... 9
Boundaries of the System ..... 14
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING ..... 15
Control Environment ..... 15
Risk Assessment Process ..... 16
Information and Communications Systems ..... 17
Monitoring Controls ..... 17
Changes to the System in the Last 12 Months ..... 17
Incidents Since the Last Review ..... 18
Criteria Not Applicable to the System ..... 18
Subservice Organizations ..... 18
COMPLEMENTARY USER ENTITY CONTROLS ..... 20
TRUST SERVICES CATEGORIES ..... 21

**SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS ..... 23**

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS ..... 24
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION ..... 25
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY ..... 25
ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY ..... 96
ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY ..... 101

**SECTION 5 OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION ..... 104**

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS ..... 105

# SECTION 1

# ASSERTION OF YANKA INDUSTRIES INC. DBA MASTERCLASS MANAGEMENT

## ASSERTION OF YANKA INDUSTRIES INC. DBA MASTERCLASS MANAGEMENT

February 16, 2026

We have prepared the accompanying description of Yanka Industries Inc. dba MasterClass' ('MasterClass' or 'the Company') MasterClass Services System titled "Yanka Industries Inc. dba MasterClass' Description of Its MasterClass Services System throughout the period January 1, 2025 to December 31, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the MasterClass Services System that may be useful when assessing the risks arising from interactions with MasterClass' system, particularly information about system controls that MasterClass has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

MasterClass uses Amazon Web Services, Inc. ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at MasterClass, to achieve MasterClass' service commitments and system requirements based on the applicable trust services criteria. The description presents MasterClass' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of MasterClass' controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. the description presents the MasterClass Services System that was designed and implemented throughout the period January 1, 2025 to December 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that MasterClass' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of MasterClass' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that MasterClass' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of MasterClass' controls operated effectively throughout that period.

Mandar Bapaye

Mandar Bapaye
CTO
Yanka Industries Inc. dba MasterClass

# SECTION 2

# INDEPENDENT SERVICE AUDITOR'S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To: Yanka Industries Inc. dba MasterClass

*Scope*

We have examined MasterClass' accompanying description of its MasterClass Services System titled "Yanka Industries Inc. dba MasterClass' Description of Its MasterClass Services System throughout the period January 1, 2025 to December 31, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that MasterClass' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

The information included in Section 5, "Other Information Provided by the Service Organization," is presented by MasterClass management to provide additional information and is not a part of the description. Information about MasterClass' management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve MasterClass' service commitments and system requirements based on the applicable trust services criteria.

*Service Organization's Responsibilities*

MasterClass 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 MasterClass' service commitments and system requirements were achieved. MasterClass has provided the accompanying assertion titled "Assertion of Yanka Industries Inc. dba MasterClass Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. MasterClass 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 the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

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

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

*Independence and Ethical Responsibilities*

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 conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

*Description of Tests of Controls*

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

*Opinion*

In our opinion, in all material respects,

a. the description presents the MasterClass Services System that was designed and implemented throughout the period January 1, 2025 to December 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that MasterClass' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of MasterClass' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that MasterClass' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of MasterClass' 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 MasterClass, user entities of the MasterClass Services System during some or all of the period January 1, 2025 to December 31, 2025, business partners of MasterClass subject to risks arising from interactions with the MasterClass 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, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- 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.

A-LIGN ASSURANCE

Tampa, Florida
February 16, 2026

# SECTION 3

# YANKA INDUSTRIES INC. DBA MASTERCLASS' DESCRIPTION OF ITS MASTERCLASS SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2025 TO DECEMBER 31, 2025

# OVERVIEW OF OPERATIONS

## Company Background

MasterClass is a premium digital learning and development platform founded in 2015 by David Rogier and Aaron Rasmussen. The founders, both experienced in the education technology industry, identified an opportunity to reimagine learning by combining world-class instruction with high-quality production and scalable technology. Their vision was to create an engaging, in-depth learning experience led by the most accomplished and recognized experts across a broad range of disciplines.

Since its founding, MasterClass has grown into a globally recognized provider of digital learning content and professional development solutions. The platform features a continually expanding library of courses taught by more than 200 internationally renowned instructors spanning business, leadership, culinary arts, writing, performing arts, design, science and technology, sports, wellness, and other subject areas.

## Description of Services Provided

MasterClass is a subscription-based platform that provides its users with access to a comprehensive catalog of video and audio learning experiences designed to support skill development, creative exploration, and professional growth. Each course consists of a structured series of professionally produced lessons led by expert instructors and may include supplementary materials such as workbooks, exercises, and applied learning activities to reinforce key concepts.

Beyond its core product-an on-demand content library, MasterClass also offers the Certificates product--defined learning paths, curated coursework, and assessments designed to build practical, job-relevant skills. These programs culminate in shareable digital certificate that demonstrates completion of the learning requirements.

MasterClass also offers the On Call product--an AI-powered coaching tool that delivers personalized guidance, contextual recommendations, and interactive role-play simulations to support real-world professional scenarios such as leadership conversations, negotiations, and performance discussions.

Most recently, MasterClass has created a new offering--MasterClass Executive, which is a scalable learning and development solutions designed to support workforce capability building and employee engagement. This product includes centralized administrative tools, user management, and reporting capabilities that enable organizations to deploy and oversee learning initiatives across teams and departments.

MasterClass and its other products operate within a cloud-based technology environment supported by formal policies, procedures, and technical controls designed to promote secure, reliable, and consistent delivery of its services.

## Principal Service Commitments and System Requirements

As a digital learning and development platform, MasterClass' primary service commitment is to deliver high-quality learning experiences led by globally recognized experts in their respective fields. The company is dedicated to producing engaging, immersive, and comprehensive content that supports skill development, creative growth, and professional advancement across a wide range of disciplines.

MasterClass operates within a cloud-based technology environment designed to support reliable content delivery, user account management, subscription services, and personalized learning experiences. The platform is built to provide a consistent, high-quality experience for individual subscribers and organizational customers while maintaining the performance, scalability, and security required to support its global user base. MasterClass services are accessible through supported web browsers on desktop and mobile devices, as well as through native applications distributed via major application stores.

**Components of the System**

*Infrastructure*

Primary infrastructure used to provide the MasterClass Services System includes the following:

| Primary Infrastructure | | |
|---|---|---|
| **Hardware** | **Type** | **Purpose** |
| Amazon Elastic Cloud Compute (EC2) | Virtualized Linux Containers | On demand, scalable cloud computing containers capable of running prebuilt user-specified images or code |
| Amazon Elastic Kubernetes Service (EKS) | Scalable Managed Kubernetes Service | Orchestration and Management of the containerized workloads and services |
| Amazon Relational Database Service (RDS) | Database Engine | Database as a Service |
| Cloudflare | Content Delivery Network (CDN) | Networking solution to optimize speed and reliability of the in-scope application |

*Software*

Primary software used to provide the MasterClass Services System includes the following:

| Primary Software | |
|---|---|
| **Software** | **Purpose** |
| New Relic | Tool used to monitor performance and uptime of the MasterClass application |
| PagerDuty | Incident Response platform integrated with New Relic and Coralogix to notify and alert Information Technology (IT) personnel of any service disruptions and outages |
| CrowdStrike | Next-generation centralized antivirus for workstations |
| JAMF Protect | Next-generation centralized antivirus for apple workstations |
| Cisco Meraki Umbrella | Security threat detection tool for workstations |
| GitHub | Cloud-based service for software development and version control |
| SonarCloud | Runs static code scans during the development process |
| JIRA | Ticketing system to document and track system changes and user access |
| Let’s Encrypt | Certificate Authority providing Transport Layer Security (TLS) certificates for the MasterClass application |

*People*

The team at MasterClass comprises individuals selected for their expertise and knowledge in their respective fields. This includes the instructors, who are contracted to teach courses on the platform, as well as other specialists who support the development and delivery of educational content. The instructors are among the most accomplished and recognized professionals in their industries, bringing their experience and insights to create entertaining, engaging, informative, and inspiring lessons.

Additionally, internal specialists work in areas such as content development, production, instructional design, information security, and compliance, playing a vital role in maintaining the high standards of MasterClass. Through their expertise and dedication, these internal professionals help ensure that MasterClass remains a leading destination for high-quality online educational entertainment.

Included in the staff are a team of support staff, such as customer service representatives and technical support personnel, to assist with any issues or questions students may have. Along with specialist instructors and support staff, employees are organized in the following functional areas:

- **Senior Management**: The Senior Management at MasterClass is a group of experienced and knowledgeable leaders who are responsible for overseeing the strategic direction and operations of the company. This team includes the company's Chief Executive Officer (CEO), Chief Financial Officer (CFO), CTO, and other executives who have been appointed to lead various departments and functions within the organization. The senior management team works closely with other members of the company to develop and implement strategies that support the growth and success of MasterClass. This team is responsible for setting the vision and goals for the company, and for making the key decisions that will shape its future. Through their leadership and expertise, the senior management team at MasterClass helps to ensure that the company remains a leader in online education.
- **People Experience**: The People Experience team at MasterClass is responsible for supporting the success of the company's internal employees and creating a positive supportive work environment for the company's employees, who were hired for their expertise and knowledge in their respective fields. This team is responsible for managing the company's Human Resources (HR) functions, including recruiting, hiring, training, and developing employees. The people experience team also works closely with managers and employees to address any issues or concerns that may arise, and to ensure that employees feel valued and supported in their work. Additionally, the people experience team is responsible for implementing programs and initiatives that support employee wellbeing and engagement, such as wellness programs and professional development opportunities. Through their efforts, the people experience team helps to foster a positive and inclusive culture at MasterClass and to support the success of the company's internal specialists.
- **Content**: The Content team at MasterClass is responsible for developing and producing the high-quality video courses offered on the platform. This team works closely with the instructors to create engaging, informative, and inspiring lessons that provide students with an in-depth learning experience. The content team is also responsible for managing the production process, from pre-production planning to post-production editing, to ensure that the courses are delivered on time and meet the high standards of MasterClass. This team plays a key role in ensuring that MasterClass remains a leading provider of online education.
- **Product**: The Product team at MasterClass is responsible for the design and development of the platform's online learning experience. This team works closely with other departments, such as the content team and the marketing team, to create a seamless and intuitive user experience that makes it easy for students to find and enroll in courses, access course materials, and interact with instructors and other students. The product team is also responsible for analyzing data and user feedback to continuously improve the platform and ensure that it meets the evolving needs of its users. Through their efforts, the product team helps to make MasterClass a leader in online education.
- **Legal**: The Legal team at MasterClass plays a crucial role in ensuring that the company operates in compliance with relevant laws and regulations. This team is responsible for providing legal advice and guidance to other departments on a wide range of issues, including contract negotiations, intellectual property, privacy, and compliance. The legal team also works closely with the content team to ensure that the courses offered on the platform do not infringe on the rights of third-parties. In addition, the legal team is responsible for managing any legal disputes or challenges that may arise. Through their expertise and diligence, the legal team helps to protect the interests of MasterClass and its stakeholders.

- **Marketing**: The Marketing team at MasterClass is responsible for promoting the platform and its courses to potential students. This team develops and implements marketing strategies and campaigns that showcase the unique features and benefits of MasterClass, and that highlight the expertise and accomplishments of the instructors who teach on the platform. The marketing team also works closely with the content and product teams to ensure that the messaging and branding of the platform is consistent and effective. Through their efforts, the marketing team helps to increase awareness of MasterClass and drive enrollment in its courses.
- **Talent and Business**: The Talent and Business teams at MasterClass are responsible for identifying and recruiting instructors who are leaders in their respective fields, and for negotiating and managing their contracts and relationships with the company. The talent team is responsible for finding and evaluating potential instructors, and for working with them to develop course outlines and lesson plans that align with the high standards of MasterClass. The business team is responsible for negotiating and managing the financial and legal aspects of the instructor relationships, and for ensuring that the courses are delivered on time and to the satisfaction of both the instructors and the students. Through their efforts, the talent and business teams help to make MasterClass a destination for the world's best instructors and their most dedicated students.
- **Finance**: The Finance team at MasterClass is responsible for managing the company's financial operations and ensuring its financial health. This team is responsible for developing and implementing financial strategies, creating and managing budgets, and analyzing data to identify trends and opportunities for growth. The finance team also works closely with other departments to ensure that the company's financial resources are allocated and used effectively. Additionally, the finance team is responsible for managing the company's relationships with investors, lenders, and other financial partners. Through their expertise and diligence, the finance team helps to ensure that MasterClass is well-positioned for long-term success.
- **Operations**: The Operations team at MasterClass is responsible for ensuring the smooth and efficient day-to-day running of the company. This team is responsible for managing the various processes and systems that are necessary for the successful delivery of the online courses offered on the platform. This includes managing the content creation and production process, overseeing the technical infrastructure and security of the platform, and coordinating with other departments to ensure that the company's operations are aligned with its strategic goals. Through their efforts, the operations team helps to ensure that MasterClass is able to deliver a high-quality learning experience to its students.
- **Infrastructure / Systems**: The Infrastructure and System teams at MasterClass are responsible for managing the technical infrastructure and systems that support the delivery of the company's online courses. This includes ensuring the stability, security, and performance of the platform, as well as implementing and maintaining the various tools and systems that are used to create, manage, and deliver the courses. The infrastructure and system teams work closely with other departments, such as the content and product teams, to ensure that the platform is able to meet the evolving needs of the company and its users. Through their expertise and diligence, the infrastructure and system teams help to ensure that MasterClass is able to deliver a high-quality and reliable learning experience to its students.
- **Information Security / Compliance**: The Information Security and Compliance teams at MasterClass are responsible for ensuring the security and compliance of the company's operations. The information security team is responsible for protecting the company's systems and data from unauthorized access, theft, or damage. This includes implementing and maintaining security measures such as firewalls, encryption, and access controls, as well as monitoring for and responding to security incidents. The compliance team is responsible for ensuring that the company's operations comply with relevant laws, regulations, and industry standards. This includes conducting audits and reviews, providing guidance and training to other departments, and managing any regulatory or legal issues that may arise. Through their expertise and diligence, the information security and compliance teams help to protect the interests of MasterClass and its stakeholders.

*Data*

MasterClass collects and processes a variety of data in order to provide its online education services. This includes personal information provided by users when they create an account on the platform, such as their name and e-mail address. MasterClass also collects data on users' interactions with the platform, such as the classes they have enrolled in and the progress they have made in those classes. This data is used to personalize the learning experience for each user and provide them with relevant recommendations and updates on their courses. Additionally, MasterClass may collect data on users' devices and browsers, such as their Internet Protocol (IP) address and information about their operating system and browser type, in order to ensure the platform is functioning properly and to improve the user experience. This data is processed in accordance with MasterClass' privacy policy and applicable laws.

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in partner contracts. Data is encrypted both in transit and at rest.

*Processes, Policies and Procedures*

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the MasterClass policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any MasterClass team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope services. Refer to the "Subservice Organizations" section below for controls managed by AWS.

Logical Access

MasterClass uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, MasterClass implements monitoring of one or more of the responsibilities. Monitoring is performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

Employees sign on to internal MasterClass resources using OneLogin, a cloud-based identity and access management provider. Users are required to use the Single Sign-On (SSO) and multi-factor authentication (MFA) services provided by OneLogin to access corporate systems. Passwords conform to defined password standards and are enforced through parameter settings in OneLogin. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user Identification's (ID)'s ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Users of the MasterClass streaming service access the platform through the Internet using the TLS functionality of their web-browser. These users supply a valid user ID and password to gain access to user resources.

On an annual basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager.

As part of this process, the CTO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

As a provider of online education services, MasterClass relies heavily on its computer systems and technology to deliver its classes and learning materials to students. To ensure the continued availability and performance of these systems, the company has implemented various processes and procedures related to computer operations backup and disaster recovery. These include things like regular backups of data and systems, redundant servers and storage systems, and disaster recovery plans in case of system failures or other disruptions. Additionally, the company has procedures in place for monitoring and maintaining the performance and security of its systems, as well as for responding to and addressing any issues that may arise. Overall, these processes and procedures are designed to ensure that MasterClass is able to provide its services without interruption, even in the event of unforeseen technical issues or disasters.

AWS is responsible for maintaining database backups that support the availability of the in-scope service.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

To ensure the availability of its computer systems and technology, MasterClass has implemented various processes and procedures. These include things like:

- Regular monitoring and maintenance of the platform and its systems to identify and address any potential issues that could impact availability.
- Redundant servers and storage systems to provide backup in case of failures or other disruptions.
- Disaster recovery plans to ensure the platform can continue to operate in the event of major disruptions or disasters.
- Regular updates and upgrades to the platform and its systems to improve performance and reliability.
- Procedures for responding to and addressing any issues or outages that may occur.

Overall, these processes and procedures are designed to ensure that MasterClass is able to provide its online education services to students without interruption.

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope services. Refer to the “Subservice Organizations” section below for controls managed by AWS.

Change Control

MasterClass follows a range of processes and procedures related to change control in order to ensure the stability and reliability of its online platform. These include:

- Establishing a formal process for requesting, reviewing, and approving changes to the platform or its systems.

- Developing a comprehensive change management plan that outlines the steps involved in implementing a change, including testing and rollout.
- Implementing strict access controls to prevent unauthorized changes to the platform or its systems.
- Conducting regular audits and reviews to ensure that changes are being implemented properly and in accordance with the change management plan.
- Providing regular updates and communication to users and stakeholders about any changes that are being made to the platform.

Overall, these processes and procedures are designed to ensure that changes to the MasterClass platform are managed in a controlled and effective manner, with minimal impact on the stability and reliability of the system.

MasterClass maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes by developers.

Data Communications

The process and procedures at MasterClass for data communications are designed to ensure the security and reliability of the company's data. This includes the use of firewall systems to control and monitor the flow of data in and out of the company's network, as well as regularly scheduled data backups to ensure that the company's data can be recovered in the event of a disaster or outage. In addition, the company conducts regular penetration testing and vulnerability scanning to identify and address any potential vulnerabilities in its systems and networks. Through these measures, the process and procedures at MasterClass for data communications help to protect the company's data and to ensure that it is able to communicate and share information securely and effectively.

**Boundaries of the System**

The scope of this report includes the MasterClass Services System performed in the San Francisco, California and Los Angeles, California facilities.

This report does not include the cloud hosting services provided by AWS at multiple facilities.

## RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

### Control Environment

*Integrity and Ethical Values*

The control environment at MasterClass is designed to support the company's commitment to integrity and ethical values. This includes the development and implementation of policies and procedures that reflect the company's code of conduct and that are designed to promote honesty, fairness, and responsibility. The control environment at MasterClass also includes training and awareness programs that help to educate employees about the company's expectations and standards, as well as regular audits and reviews to ensure that the policies and procedures are being followed and are effective.

Through these measures, the control environment at MasterClass helps to create a culture of integrity and ethical behavior, and to protect the interests of the company and its stakeholders.

Specific control activities that the service organization has implemented in this area are described below:

- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

*Commitment to Competence*

The control environment at MasterClass includes a commitment to competence, which means that the company recognizes the value of hiring and developing knowledgeable and skilled employees who are able to perform their jobs effectively and efficiently. To support this commitment, the company provides training and development opportunities to its employees and encourages them to continue learning and growing in their careers. The control environment at MasterClass also includes performance management processes that are designed to help employees understand their roles and responsibilities, and to provide feedback and support to help them improve their skills and knowledge. Through these measures, the control environment at MasterClass helps to ensure that the company has a competent and capable workforce, and that its employees are able to contribute to the success of the company.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

*Management's Philosophy and Operating Style*

The control environment at MasterClass includes management's philosophy and operating style, which are the guiding principles and practices that shape the way the company is run. The management team at MasterClass believes in fostering a culture of collaboration, innovation, accountability, security, and compliance and they strive to create an environment in which employees are empowered to take ownership of their work and to contribute their ideas and expertise. The management team also operates in a transparent and open manner, and they encourage open communication and feedback from employees at every level. Through these practices, the management team at MasterClass sets the tone for the control environment and helps to ensure that the company is able to operate effectively and efficiently.

*Organizational Structure and Assignment of Authority and Responsibility*

The control environment at MasterClass includes an organizational structure and assignment of authority and responsibility that are designed to support the company's operations and objectives. The organizational structure at MasterClass is hierarchical, with clear lines of authority and communication, and it is designed to provide employees with the support and resources they need to perform their jobs effectively. The assignment of authority and responsibility is based on the principle of delegation, which means that managers are empowered to make decisions and take action within the scope of their responsibilities, while being held accountable for their actions and decisions. Through these practices, the control environment at MasterClass helps to ensure that the company's operations are organized and coordinated, and that employees are able to work efficiently and effectively.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

*Human Resources Policies and Practices*

The control environment at MasterClass includes HR policies and procedures that are designed to support the company's commitment to its employees. The HR policies at MasterClass cover a range of topics, including hiring and training, performance management, compensation and benefits, and workplace safety and health. These policies are designed to provide employees with clear guidance and expectations, and to support their development and success. The HR procedures at MasterClass are the specific steps and processes that are used to implement the policies and to ensure that they are followed consistently and effectively. Through these measures, the control environment at MasterClass helps to ensure that the company is able to attract, retain, and develop a talented and engaged workforce.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

**Risk Assessment Process**

The risk assessment process at MasterClass is a systematic and ongoing process that is designed to identify and evaluate the risks that the company faces. This process involves identifying potential risks, analyzing their likelihood and impact, and developing strategies to mitigate or manage those risks. The risk assessment process at MasterClass is carried out by a team of specialists who have the knowledge and skills to identify and assess a wide range of risks, including financial, operational, legal, and reputational risks.

The team uses a variety of tools and techniques, such as scenario analysis, risk modeling, and benchmarking, to identify and evaluate the risks that the company faces. Through the risk assessment process, MasterClass is able to identify potential threats and opportunities, and to develop strategies to manage and mitigate those risks.

*Integration with Risk Assessment*

The environment in which the system operates; the commitments, agreements, and responsibilities of the MasterClass Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. MasterClass addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique.

As part of the design and operation of the system, MasterClass' management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

**Information and Communications Systems**

Information and communication is an integral component of MasterClass' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of IT. At MasterClass, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, All-hands meetings are held weekly in each geographic location and/or remotely to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the All-hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues.

General updates to entity-wide security policies and procedures are usually communicated to the appropriate MasterClass personnel via e-mail messages.

Specific information systems used to support the MasterClass Services System are described in the Description of Services section above.

**Monitoring Controls**

MasterClass has processes and systems that are used to monitor and assess the effectiveness and efficiency of the company's operations and controls. These monitoring controls are designed to provide management with timely and accurate information about the company's performance, and to identify any issues or discrepancies that may need to be addressed.

*On-Going Monitoring*

The monitoring controls at MasterClass include a range of tools and techniques, such as performance metrics, audits and reviews, and exception reporting, which are used to collect and analyze data about the company's operations. Through these monitoring controls, MasterClass is able to assess the effectiveness of its controls and to identify areas for improvement, helping to ensure the success and sustainability of the company.

*Reporting Deficiencies*

Reporting deficiencies at MasterClass refers to the process of identifying and reporting any issues or concerns that may affect the effectiveness or efficiency of the company's operations or controls. This process involves identifying potential deficiencies, evaluating their impact, and communicating the findings to the appropriate stakeholders. The reporting of deficiencies at MasterClass is an important part of the company's internal control system, and it is designed to support the identification and resolution of any issues or concerns that may affect the company's operations or objectives. Through the reporting of deficiencies, MasterClass is able to maintain the effectiveness and integrity of its controls, and to ensure that the company is able to operate in a manner that is consistent with its policies and objectives.

**Changes to the System in the Last 12 Months**

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

**Incidents Since the Last Review**

AWS US-EAST-1 Outage: On October 20, 2025, starting at 12:38 AM PDT, MasterClass experienced a service disruption affecting Persona feedback generation due to a widespread AWS outage in the US-EAST-1 region. Users attempting to generate AI feedback experienced 60-second timeouts with no feedback displayed. A postmortem report was created to include root cause, which was an AWS DynamoDB DNS race condition that cascaded to affect AWS services MasterClass' systems depend on. While MasterClass' services began auto-recovering around 4:23 AM as AWS restored endpoints, the team made the decision to hold deployments for 24 hours due to ongoing EC2 instance launch failures that persisted until 1:50 PM. The incident required minimal engineering intervention as recovery was dependent on AWS infrastructure restoration.

Cloudflare Outag: On November 18, 2025, and on December 5, 2025: During Q4 2025, MasterClass had service disruptions because of two major Cloudflare outages impacting global network and security infrastructure. Because these incidents originated within Cloudflare's own systems, it was outside of MasterClass operational control. While MasterClass actively monitored the situation and validated that the internal systems were functioning as expected, MasterClass deemed that it was not needed to directly resolve or remediate the issue. Restoration required Cloudflare to identify the root cause, roll back the faulty configuration change, and recover impacted services.

**Criteria Not Applicable to the System**

All Common/Security, Availability, and Confidentiality criteria were applicable to the MasterClass MasterClass Services System.

**Subservice Organizations**

This report does not include the cloud hosting services provided by AWS at multiple facilities.

*Subservice Description of Services*

AWS provides cloud hosting services, which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

*Complementary Subservice Organization Controls*

MasterClass' services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to MasterClass' services to be solely achieved by MasterClass control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of MasterClass.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria described within this report are met:

| **Subservice Organization - AWS** | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security | CC6.4, CC6.7 | Physical access to data centers is approved by an authorized individual. |
| | | Physical access is revoked within 24 hours of the employee or vendor record being deactivated. |

| Subservice Organization - AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. |
| | | Electronic Intrusion Detection Systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. |
| | CC6.1, CC6.4 | Recovery key materials used for disaster recovery processes by Key Management Service (KMS) are physically secured offline so that no single AWS employee can gain access to the key material. |
| | | Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes. |
| | CC6.4 | Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. |
| | | Physical access points to server locations are managed by electronic access control devices. |
| Availability | A1.2 | Amazon-owned data centers are protected by fire detection and suppression systems. |
| | | Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels. |
| | | Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers. |
| | | Amazon-owned data centers have generators to provide backup power in case of electrical failure. |
| | | Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies. |
| | | AWS performs annual reviews of colocation service providers to validate adherence with AWS security and operational standards. |
| | | Simple Storage Service (S3) performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption. |
| | | When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy. |
| | | Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution. |
| | | Critical AWS system components are replicated across multiple Availability Zones and backups are maintained. |

| Subservice Organization - AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | A1.2, C1.1 | Objects are stored redundantly across multiple fault-isolated facilities. |
| | | The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service. |
| | | If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery. |
| | | Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics. |
| | A1.2, A1.3, C1.1 | Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones. |

MasterClass' management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as Service Level Agreements (SLAs). In addition, MasterClass performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

**COMPLEMENTARY USER ENTITY CONTROLS**

MasterClass' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to MasterClass' services to be solely achieved by MasterClass control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of MasterClass.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to MasterClass.
2. User entities are responsible for notifying MasterClass of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of MasterClass services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize MasterClass services.
6. User entities are responsible for providing MasterClass with a list of approvers for security and system configuration changes for data transmission.

7. User entities are responsible for immediately notifying MasterClass of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

## TRUST SERVICES CATEGORIES

*In-Scope Trust Services Categories*

| **Common Criteria (to the Security, Availability, and Confidentiality Categories*)*** |
|---|
| Security refers to the protection of:<br>i. information during its collection or creation, use, processing, transmission, and storage and<br>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** |
|---|
| 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. |

| **Confidentiality** |
|---|
| 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 (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.<br><br>Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property. |

*Control Activities Specified by the Service Organization*

The applicable Trust Services Criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable Trust Services Criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of MasterClass' description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at MasterClass are described within Section 4 and within the Subservice Organization and Criteria Not Applicable to the System sections above.

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

# SECTION 4

# TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

## GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of MasterClass was limited to the Trust Services Criteria, related criteria and control activities specified by the management of MasterClass and did not encompass all aspects of MasterClass' operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

| TEST | DESCRIPTION |
|---|---|
| Inquiry | The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information. |
| Observation | The service auditor observed application of the control activities by client personnel. |
| Inspection | The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities. |
| Re-performance | The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control. |

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria

## CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC1.1 | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. | Inspected the entity's website and the whistleblower channel to determine that the company established a formalized whistleblower policy, and an anonymous communication channel was in place for users to report potential issues or fraud concerns. | No exceptions noted. |
| | | The company performs background checks on new employees. | Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check. | No exceptions noted. |
| | | The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Inspected the Employee Handbook and Human Resources Security Policy and the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that the company required employees to acknowledge a code of conduct at the time of hire which defined that employees who violated the code of conduct were subject to disciplinary actions in accordance with a disciplinary policy. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company requires employees to sign a confidentiality agreement during onboarding. | Inspected the signed confidentiality agreement for a sample of new hires to determine that the company required and obtained signed confidentiality agreements from all employees during their onboarding process. | No exceptions noted. |
| | | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected the completed performance evaluation tracking tool for a sample of current employees to determine that company managers were required to complete performance evaluations for direct reports at least annually. | No exceptions noted. |
| CC1.2 | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |
| | | The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed. | Inspected the board meeting minutes for a sample of quarters to determine that the company's board members had sufficient expertise to oversee management's ability to design, implement and operate information security controls. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company. | Inspected the annual board of directors meeting minutes to determine that the company's board of directors met at least annually and maintained formal meeting minutes. The board included directors that were independent of the company. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |
| | | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected the completed performance evaluation tracking tool for a sample of current employees to determine that company managers were required to complete performance evaluations for direct reports at least annually. | No exceptions noted. |
| CC1.3 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected the job description for a sample of job roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company. | Inspected the annual board of directors meeting minutes to determine that the company's board of directors met at least annually and maintained formal meeting minutes. The board included directors that were independent of the company. | No exceptions noted. |
| | | The company maintains an organizational chart that describes the organizational structure and reporting lines. | Inspected the company organization chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines. | No exceptions noted. |
| | | The company has a vendor management program in place. Components of this program include:<br>• Critical third-party vendor inventory<br>• Vendor's security and privacy requirements<br>• Review of critical third-party vendors at least annually | Inspected the third-party risk management policy, vendor inventory listing, and vendor security reviews for a sample of third-party vendors to determine that the program included requirements for:<br>• Critical third-party inventory<br>• Vendor's security and privacy requirements<br>• Review of third-party vendors at least annually | No exceptions noted. |
| CC1.4 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | Policies and procedures are in place that outline the talent acquisition, performance evaluation and annual training processes. | Inspected the Human Resource Security Policy to determine that policies and procedures were in place that outlined the talent acquisition, performance evaluation and annual training processes. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The organization evaluates the competencies and experience of candidates prior to hiring. | Inspected the employee evaluation scorecards for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring. | No exceptions noted. |
| | | The company performs background checks on new employees. | Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check. | No exceptions noted. |
| | | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected the completed performance evaluation tracking tool for a sample of current employees to determine that company managers were required to complete performance evaluations for direct reports at least annually. | No exceptions noted. |
| | | The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Inquired of the Risk Program Manager regarding security awareness training to determine that employees were required to complete security awareness training within thirty days of hire and at least annually thereafter. | No exceptions noted. |
| | | | Inspected the Human Resources Security Policy to determine that employees were required to complete security awareness training within thirty days of hire and at least annually thereafter. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the training completion logs for a sample of current employees to determine that employees were required to complete security awareness training at least annually. | No exceptions noted. |
| | | | Inspected the training completion logs for a sample of new hires to determine that employees were required to complete security awareness training within thirty days of hire. | Testing of the control activity disclosed that security awareness training was not completed within thirty days of hire for 1 of 10 new hires sampled. Subsequent testing of the control activity disclosed that security awareness training was completed after 30 days of hire. |
| | | The company has a vendor management program in place. Components of this program include:<br>• Critical third-party vendor inventory<br>• Vendor's security and privacy requirements<br>• Review of critical third-party vendors at least annually | Inspected the third-party risk management policy, vendor inventory listing, and vendor security reviews for a sample of third-party vendors to determine that the program included requirements for:<br>• Third-party inventory<br>• Vendor's security and privacy requirements<br>• Review of third-party vendors at least annually | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC1.5 | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected the job description for a sample of job roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions. | No exceptions noted. |
| | | The company maintains an organizational chart that describes the organizational structure and reporting lines. | Inspected the company organization chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines. | No exceptions noted. |
| | | The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Inspected the Employee Handbook and Human Resources Security Policy and the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that the company required employees to acknowledge a code of conduct at the time of hire which defined that employees who violated the code of conduct were subject to disciplinary actions in accordance with a disciplinary policy. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected the completed performance evaluation tracking tool for a sample of current employees to determine that company managers were required to complete performance evaluations for direct reports at least annually. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC2.1 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | Edit checks are in place to prevent incomplete or incorrect data from being entered into the system. | Inquired of the Risk Program Manager regarding edit checks to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system. | No exceptions noted. |
| | | | Observed personnel enter information into the in-scope system to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system. | No exceptions noted. |
| | | | Inspected system edit check configurations to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system. | No exceptions noted. |
| | | Accurate diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system. | Inspected the entity's data flow diagrams to determine that accurate diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system. | No exceptions noted. |
| | | Data that is entered into the system, processed by the system and output from the system is protected from unauthorized access. | Inspected code repository configurations, the IPS configurations, the encryption methods and configurations, and the VPN authentication configurations to determine that data that was entered into the system, processed by the system and output from the system was protected from unauthorized access. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | The company performs control self-assessments bi-weekly to gain assurance that controls are in place and operating effectively, corrective actions are taken based on relevant findings, and if the company has committed to an SLA for a finding, the corrective action is completed within that SLA. | Inspected the security working group meeting minutes for a sample of weeks to determine that the company performed control self-assessments bi-weekly to gain assurance that controls were in place and operating effectively, corrective actions were taken based on relevant findings, and if the company had committed to an SLA for a finding, the corrective action was completed within that SLA. | 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. | The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. | Inspected the entity's website and the whistleblower channel to determine that the company established a formalized whistleblower policy, and an anonymous communication channel was in place for users to report potential issues or fraud concerns. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected the job description for a sample of job roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions. | No exceptions noted. |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | The company communicates system changes to authorized internal users. | Inspected internal communication channel and the entity's website to determine that the company communicates system changes to authorized internal users. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Inspected the Employee Handbook and Human Resources Security Policy and the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that the company required employees to acknowledge a code of conduct at the time of hire which defined that employees who violated the code of conduct were subject to disciplinary actions in accordance with a disciplinary policy. | No exceptions noted. |
| | | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected the incident response plan to determine that security and privacy incident response policies and procedures were documented and communicated to authorized users. | No exceptions noted. |
| | | The company provides a description of its products and services to internal and external users. | Inspected the entity's website to determine that the company provided a description of its products and services to internal and external users. | No exceptions noted. |
| | | The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Inquired of the Risk Program Manager regarding security awareness training to determine that employees were required to complete security awareness training within thirty days of hire and at least annually thereafter. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the Human Resources Security Policy to determine that employees were required to complete security awareness training within thirty days of hire and at least annually thereafter. | No exceptions noted. |
| | | | Inspected the training completion logs for a sample of current employees to determine that employees were required to complete security awareness training at least annually. | No exceptions noted. |
| | | | Inspected the training completion logs for a sample of new hires to determine that employees were required to complete security awareness training within thirty days of hire. | Testing of the control activity disclosed that security awareness training was not completed within thirty days of hire for 1 of 10 new hires sampled. Subsequent testing of the control activity disclosed that security awareness training was completed after 30 days of hire. |
| CC2.3 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | Changes to commitments, requirements and responsibilities related to security, availability and confidentiality are communicated to third-parties, external users, and customers. | Inspected the entity's e-mail communications to external users to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. | Inspected the entity's website to determine that the company had an external-facing support system in place that allowed users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. | No exceptions noted. |
| | | The company notifies customers of critical system changes that may affect their processing. | Inspected the entity's website and an example e-mail notification to determine that the company notifies customers of critical system changes that may affect their processing. | No exceptions noted. |
| | | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected the incident response plan to determine that security and privacy incident response policies and procedures were documented and communicated to authorized users. | No exceptions noted. |
| | | The company's security commitments are communicated to customers in Master Service Agreements (MSAs). | Inspected the Publicly Available Terms of Service and the executed customer agreements for a sample of customers to determine that the company's security commitments were communicated to customers in MSAs. | No exceptions noted. |
| | | The company provides guidelines and technical support resources relating to system operations to customers. | Inspected the entity's website and publicly available documentation to determine that the company provided guidelines and technical support resources relating to system operations to customers. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company provides a description of its products and services to internal and external users. | Inspected the entity's website to determine that the company provided a description of its products and services to internal and external users. | No exceptions noted. |
| | | The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Inspected the third-party risk management policy and the executed third-party agreements for a sample of third-parties to determine that the company had written agreements in place with vendors and related third-parties, and these agreements included confidentiality and privacy commitments applicable to that entity. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC3.1 | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |
| | | The company maintains an organizational chart that describes the organizational structure and reporting lines. | Inspected the company organization chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company specifies its objectives to enable the identification and assessment of risk related to the objectives. | Inspected the security risk management program and the Security Working Group meeting minutes for a sample of weeks to determine that the company specified its objectives to enable the identification and assessment of risk related to the objective. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | The annual comprehensive risk assessment results are reviewed and approved by management. | Inspected the security risk management program and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by management. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a vendor management program in place. Components of this program include:<br>• Critical third-party vendor inventory<br>• Vendor's security and privacy requirements<br>• Review of critical third-party vendors at least annually | Inspected the third-party risk management policy, vendor inventory listing, and vendor security reviews for a sample of third-party vendors to determine that the program included requirements for:<br>• Third-party inventory<br>• Vendor's security and privacy requirements<br>• Review of third-party vendors at least annually | No exceptions noted. |
| CC3.3 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC3.4 | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a vendor management program in place. Components of this program include:<br>• Critical third-party vendor inventory<br>• Vendor's security and privacy requirements<br>• Review of critical third-party vendors at least annually | Inspected the third-party risk management policy, vendor inventory listing, and vendor security reviews for a sample of third-party vendors to determine that the program included requirements for:<br>• Third-party inventory<br>• Vendor's security and privacy requirements<br>• Review of third-party vendors at least annually | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Alerts are sent to appropriate personnel who have the authority to react to the alert. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity, and alerts were sent to appropriate personnel who have the authority to react to the alert. | No exceptions noted. |
| | | The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it annually. | Inspected the business continuity and disaster recovery policy and the completed tabletop exercise test results to determine that business continuity/disaster recovery plans were documented and tested annually. | No exceptions noted. |
| | | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |
| | | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected the completed performance evaluation tracking tool for a sample of current employees to determine that company managers were required to complete performance evaluations for direct reports at least annually. | No exceptions noted. |
| | | The company conducts access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes are tracked to completion. | Inquired of the IT Manager regarding access reviews to determine that the company conducted access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes were tracked to completion. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected a completed access review for the in-scope systems to determine that the company conducted access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes were tracked to completion. | No exceptions noted. |
| | | The company performs control self-assessments bi-weekly to gain assurance that controls are in place and operating effectively, corrective actions are taken based on relevant findings, and if the company has committed to an SLA for a finding, the corrective action is completed within that SLA. | Inspected the security working group meeting minutes for a sample of weeks to determine that the company performed control self-assessments bi-weekly to gain assurance that controls were in place and operating effectively, corrective actions were taken based on relevant findings, and if the company had committed to an SLA for a finding, the corrective action was completed within that SLA. | No exceptions noted. |
| | | The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. | Inspected the completed penetration test report to determine that penetration testing was performed at least annually. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a vendor management program in place. Components of this program include:<br>• Critical third-party vendor inventory<br>• Vendor's security and privacy requirements<br>• Review of critical third-party vendors at least annually | Inspected the third-party risk management policy, vendor inventory listing, and vendor security reviews for a sample of third-party vendors to determine that the program included requirements for:<br>• Third-party inventory<br>• Vendor's security and privacy requirements<br>• Review of third-party vendors at least annually | No exceptions noted. |
| | | Host-based vulnerability scans are performed on a continuous basis on all external-facing systems and critical and high vulnerabilities are tracked to remediation. | Inspected the operations security policy and a sample of completed vulnerability scan results and associated remediation tickets to determine that host-based vulnerability scans were performed on a continuous basis on all external-facing systems and critical and high vulnerabilities were tracked to remediation. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test 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. | The annual comprehensive risk assessment results are reviewed and approved by management. | Inspected the security risk management program and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by management. | No exceptions noted. |
| | | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company performs control self-assessments bi-weekly to gain assurance that controls are in place and operating effectively, corrective actions are taken based on relevant findings, and if the company has committed to an SLA for a finding, the corrective action is completed within that SLA. | Inspected the security working group meeting minutes for a sample of weeks to determine that the company performed control self-assessments bi-weekly to gain assurance that controls were in place and operating effectively, corrective actions were taken based on relevant findings, and if the company had committed to an SLA for a finding, the corrective action was completed within that SLA. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Management has documented and incorporated controls into the environment that include manual, automated, preventive, detective, and corrective controls to reduce risks of control and system failure. | Inspected the list of controls within the compliance automation software to determine that management had documented and incorporated controls into the environment that included manual, automated, preventive, detective, and corrective controls to reduce risks of control and system failure. | No exceptions noted. |
| | | The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | Inspected the business continuity and disaster recovery policy to determine that business continuity and disaster recovery plans were documented that outlined communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | No exceptions noted. |
| | | The company has a documented business continuity/disaster recovery plan and tests it annually. | Inspected the business continuity and disaster recovery policy and the completed tabletop exercise test results to determine that BC/DR plans were documented and tested annually. | No exceptions noted. |
| | | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company. | Inspected the annual board of directors meeting minutes to determine that the company's board of directors met at least annually and maintained formal meeting minutes. The board included directors that were independent of the company. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | 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. | The internal controls implemented around the entity's technology infrastructure include, but are not limited to:<br>• Restricting access rights to authorized users<br>• Limiting services to what is required for business operations<br>• Authentication of access<br>• Protecting the entity's assets from external threats | Inspected the list of controls within the compliance automation software to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to:<br>• Restricting access rights to authorized users<br>• Limiting services to what was required for business operations<br>• Authentication of access<br>• Protecting the entity's assets from external threats | No exceptions noted. |
| | | Management has documented and incorporated controls into the environment that include manual, automated, preventive, detective, and corrective controls to reduce risks of control and system failure. | Inspected the list of controls within the compliance automation software to determine that management had documented and incorporated controls into the environment that included manual, automated, preventive, detective, and corrective controls to reduce risks of control and system failure. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | 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. | Management has documented and incorporated controls into the environment that include manual, automated, preventive, detective, and corrective controls to reduce risks of control and system failure. | Inspected the list of controls within the compliance automation software to determine that management had documented and incorporated controls into the environment that included manual, automated, preventive, detective, and corrective controls to reduce risks of control and system failure. | No exceptions noted. |
| | | On at least a bi-weekly basis, the company's board of directors or a relevant subcommittee is briefed by senior management on the state of the company's cybersecurity and privacy risk and the board provides feedback and direction to management as needed. | Inspected the security working group meeting minutes for a sample of weeks to determine that on at least a bi-weekly basis, the board of directors or a relevant subcommittee was briefed by senior management on the state of the company's cybersecurity and privacy risk, and the board provided feedback and direction to management as needed. | No exceptions noted. |
| | | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected the job description for a sample of job roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected the job description for a sample of key security roles to determine that company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC6.1 | The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | Administrative access is restricted to appropriate user accounts for the network, VPN, application, and database. | Inquired of the IT Manager regarding administrative access to determine that administrative access was restricted to appropriate user accounts at the network, application, and database layers. | No exceptions noted. |
| | | | Inspected the listings of administrative users to the network, application, database, and VPN to determine that administrative access was restricted to appropriate user accounts for the network, VPN application, and database. | No exceptions noted. |
| | | Data entering the environment is secured and monitored through the use of firewalls and an IPS. | Inspected IPS configurations, the firewall rule sets and the network diagram to determine that data entering the environment was secured and monitored through the use of firewalls and an IDS. | No exceptions noted. |
| | | The company assigns a unique name and number for identifying and tracking user identity. | Inspected the network, VPN, application, and database user listings to determine that users were assigned a unique name and number for identifying and tracking user identity. | No exceptions noted. |
| | | The company has implemented procedures for creating, changing, and safeguarding passwords. | Inspected encryption configurations for data at rest and password encryption configurations to determine that the company implemented procedures for creating, changing, and safeguarding passwords. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Inquired of the IT Manager regarding procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to determine that the company implemented procedures to regularly review the respective records of information system activity. | No exceptions noted. |
| | | | Inspected the network, application, database, and VPN audit logging configurations and an example audit log extract to determine that the company implemented procedures to review records of information system activity. | No exceptions noted. |
| | | The company maintains a formal inventory of production system assets. | Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets. | No exceptions noted. |
| | | The company restricts access to migrate changes to production to authorized personnel. | Inquired of the IT Manager regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| Logical and Physical Access Controls | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized personnel. | No exceptions noted. |
| | | The company restricts privileged access to encryption keys to authorized users with a business need. | Inspected the cryptography policy, the access control and asset management policy, and the encryption configurations for data at rest to determine that privileged access to encryption keys was restricted to authorized users with a business need. | No exceptions noted. |
| | | The company's datastores housing sensitive customer data are encrypted at rest. | Inspected encryption configurations for data at rest to determine that datastores housing sensitive customer data were encrypted at rest. | No exceptions noted. |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | System access restricted to authorized access only. | Inquired of the IT Manager regarding system access to determine that system access was restricted to authorized access only. | No exceptions noted. |
| | | | Inspected the application and VPN administrator listing to determine that system access was restricted to authorized access only. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company requires authentication to the "production network" to use unique usernames and passwords. | Inspected the network user listing and the network password configurations to determine that the company required authentication to the "production network" to use unique usernames and passwords. | No exceptions noted. |
| | | The company requires passwords for in-scope system components to be configured according to the company's policy. | Inspected the network, application, database, and VPN password settings to determine that passwords for in-scope system components were configured according to the company's policy. | No exceptions noted. |
| | | The company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method. | Inquired of the Risk Program Manager regarding user authentication to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | | Observed a user authenticate to the VPN access to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | | Inspected the VPN authentication settings to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company restricts privileged access to databases to authorized users with a business need. | Inquired of the IT Manager regarding access to stored data to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | | Inspected the database user listing, admin listing, and access rights to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | The company restricts privileged access to the firewall to authorized users with a business need. | Inspected the firewall admin listing to determine that privileged access to the firewall was restricted to authorized users with a documented business need. | No exceptions noted. |
| | | The company restricts privileged access to the production network to authorized users with a business need. | Inquired of the IT Manager regarding privileged access to determine that the company restricted privileged access to the production network to authorized users with a business need. | No exceptions noted. |
| | | | Inspected the network administrator listing to determine that the company restricted privileged access to the production network to authorized users with a business need. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Inquired of the IT Security Manager regarding the termination procedures to determine that the company completed termination checklists to ensure that access was revoked for terminated employees within SLAs. | No exceptions noted. |
| | | | Inspected the termination procedures, network, application, database, and VPN user listings, and the access revocation ticket for a sample of terminated employees to determine that the company completes termination checklists to ensure that access was revoked for terminated employees within SLAs. | No exceptions noted. |
| | | The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Inspected the access request ticket for a sample of new hires to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. | Inspected the network, application, database, and VPN audit logging configurations and an example audit log extract to determine that the company utilized a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. | No exceptions noted. |
| | | The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Inspected encryption configurations for data in transit and the password encryption configurations to determine that the company enforced secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | | The company's network is segmented to prevent unauthorized access to customer data. | Inspected the network diagram, the network segregation diagrams, and the firewall rulesets to determine that the entity's various networks were segmented to prevent unauthorized access to customer data. | No exceptions noted. |
| | | The company uses firewalls and configures them to prevent unauthorized access. | Inspected the network diagram and firewall rule sets for the production environment to determine that a firewall was in place to prevent unauthorized access. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |
| 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. | Administrative access is restricted to appropriate user accounts for the network, VPN, application, and database. | Inquired of the IT Manager regarding administrative access to determine that administrative access was restricted to appropriate user accounts at the network, application, and database layers. | No exceptions noted. |
| | | | Inspected the listings of administrative users to the network, application, database, and VPN to determine that administrative access was restricted to appropriate user accounts for the network, VPN application, and database. | No exceptions noted. |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |
| | | The company requires authentication to the “production network” to use unique usernames and passwords. | Inspected the network user listing and the network password configurations to determine that the company required authentication to the "production network" to use unique usernames and passwords. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company conducts access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes are tracked to completion. | Inquired of the IT Manager regarding access reviews to determine that the company conducted access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes were tracked to completion. | No exceptions noted. |
| | | | Inspected a completed access review for the in-scope systems to determine that the company conducted access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes were tracked to completion. | No exceptions noted. |
| | | The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Inquired of the IT Security Manager regarding the termination procedures to determine that the company completed termination checklists to ensure that access was revoked for terminated employees within SLAs. | No exceptions noted. |
| | | | Inspected the termination procedures, network, application, database, and VPN user listings, and the access revocation ticket for a sample of terminated employees to determine that the company completes termination checklists to ensure that access was revoked for terminated employees within SLAs. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Inspected the access request ticket for a sample of new hires to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | 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. | Administrative access is restricted to appropriate user accounts for the network, VPN, application, and database. | Inquired of the IT Manager regarding administrative access to determine that administrative access was restricted to appropriate user accounts at the network, application, and database layers. | No exceptions noted. |
| | | | Inspected the listings of administrative users to the network, application, database, and VPN to determine that administrative access was restricted to appropriate user accounts for the network, VPN application, and database. | No exceptions noted. |
| | | The company assigns a unique name and number for identifying and tracking user identity. | Inspected the network, VPN, application, and database user listings to determine that users were assigned a unique name and number for identifying and tracking user identity. | No exceptions noted. |
| | | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected the information security policies and procedures to determine that information security policies and procedures were documented and reviewed at least annually. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | System access restricted to authorized access only. | Inquired of the IT Manager regarding system access to determine that system access was restricted to authorized access only. | No exceptions noted. |
| | | | Inspected the application and VPN administrator listing to determine that system access was restricted to authorized access only. | No exceptions noted. |
| | | The company requires authentication to the “production network” to use unique usernames and passwords. | Inspected the network user listing and the network password configurations to determine that the company required authentication to the "production network" to use unique usernames and passwords. | No exceptions noted. |
| | | The company restricts privileged access to databases to authorized users with a business need. | Inquired of the IT Manager regarding access to stored data to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | | Inspected the database user listing, admin listing, and access rights to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | The company restricts privileged access to the production network to authorized users with a business need. | Inquired of the IT Manager regarding privileged access to determine that the company restricted privileged access to the production network to authorized users with a business need. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the network administrator listing to determine that the company restricted privileged access to the production network to authorized users with a business need. | No exceptions noted. |
| | | The company conducts access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes are tracked to completion. | Inquired of the IT Manager regarding access reviews to determine that the company conducted access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes were tracked to completion. | No exceptions noted. |
| | | | Inspected a completed access review for the in-scope systems to determine that the company conducted access reviews semi-annually for the in-scope system components to help ensure that access is restricted appropriately and required changes were tracked to completion. | No exceptions noted. |
| | | The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Inquired of the IT Security Manager regarding the termination procedures to determine that the company completed termination checklists to ensure that access was revoked for terminated employees within SLAs. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the termination procedures, network, application, database, and VPN user listings, and the access revocation ticket for a sample of terminated employees to determine that the company completes termination checklists to ensure that access was revoked for terminated employees within SLAs. | No exceptions noted. |
| | | The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Inspected the access request ticket for a sample of new hires to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | 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. | This criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. | Inspected the data management and retention policy and the destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that the company had electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed. | No exceptions noted. |
| | | The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | Inspected the data management and retention policies and procedures to determine that policies and procedures were in place to guide the secure retention and disposal of company and customer data. | No exceptions noted. |
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | The company assigns a unique name and number for identifying and tracking user identity. | Inspected the network, VPN, application, and database user listings to determine that users were assigned a unique name and number for identifying and tracking user identity. | No exceptions noted. |
| | | The company's datastores housing sensitive customer data are encrypted at rest. | Inspected encryption configurations for data at rest to determine that datastores housing sensitive customer data were encrypted at rest. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. | Inspected the centralized antivirus software dashboard console and the centralized antivirus configurations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configured to be updated routinely, logged, and installed on all relevant systems. | No exceptions noted. |
| | | The company requires authentication to the “production network” to use unique usernames and passwords. | Inspected the network user listing and the network password configurations to determine that the company required authentication to the "production network" to use unique usernames and passwords. | No exceptions noted. |
| | | The company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method. | Inquired of the Risk Program Manager regarding user authentication to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | | Observed a user authenticate to the VPN access to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the VPN authentication settings to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | Inspected encryption configurations for data in transit and the VPN authentication configurations to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | No exceptions noted. |
| | | The company restricts privileged access to databases to authorized users with a business need. | Inquired of the IT Manager regarding access to stored data to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | | Inspected the database user listing, admin listing, and access rights to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Inspected encryption configurations for data in transit and the password encryption configurations to determine that the company enforced secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | | The company uses firewalls and configures them to prevent unauthorized access. | Inspected the network diagram and firewall rule sets for the production environment to determine that a firewall was in place to prevent unauthorized access. | 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. | The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails. | Inspected the backup replication configurations and an example backup replication completion log to determine that the company's databases were replicated to a secondary data center on a real-time basis, and alerts were configured to notify administrators if replication failed. | No exceptions noted. |
| | | The company encrypts portable and removable media devices when used. | Inspected the encryption configurations for data at rest to determine that the company encrypts portable and removable media devices when used. | No exceptions noted. |
| | | The company's datastores housing sensitive customer data are encrypted at rest. | Inspected encryption configurations for data at rest to determine that datastores housing sensitive customer data were encrypted at rest. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method. | Inquired of the Risk Program Manager regarding user authentication to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | | Observed a user authenticate to the VPN access to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | | Inspected the VPN authentication settings to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method. | No exceptions noted. |
| | | The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | Inspected encryption configurations for data in transit and the VPN authentication configurations to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | No exceptions noted. |
| | | The company restricts privileged access to databases to authorized users with a business need. | Inquired of the IT Manager regarding access to stored data to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the database user listing, admin listing, and access rights to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. | Inspected the encryption configurations for mobile devices to determine that an MDM system was in place to centrally manage mobile devices supporting the service. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |
| | | The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Inspected encryption configurations for data in transit and the password encryption configurations to determine that the company enforced secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | | The company uses firewalls and configures them to prevent unauthorized access. | Inspected the network diagram and firewall rule sets for the production environment to determine that a firewall was in place to prevent unauthorized access. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |
| 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. | Data entry points are secured. | Inspected code repository configurations to determine that code repository software was in place to ensure only authorized changes were deployed into the production environment. | No exceptions noted. |
| | | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected code repository configurations and an example alert generated from the code repository to determine that the code repository software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Alerts are sent to appropriate personnel who have the authority to react to the alert. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity, and alerts were sent to appropriate personnel who have the authority to react to the alert. | No exceptions noted. |
| | | The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected the change management and secure development policies and procedures to determine that the company had a formal SDLC methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access Controls** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. | Inspected the centralized antivirus software dashboard console and the centralized antivirus configurations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configured to be updated routinely, logged, and installed on all relevant systems. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |
| | | An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Data entry points are secured. | Inspected code repository configurations to determine that code repository software was in place to ensure only authorized changes were deployed into the production environment. | No exceptions noted. |
| | | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected code repository configurations and an example alert generated from the code repository to determine that the code repository software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Alerts are sent to appropriate personnel who have the authority to react to the alert. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity, and alerts were sent to appropriate personnel who have the authority to react to the alert. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. | Inspected the completed penetration test report to determine that penetration testing was performed at least annually. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |
| | | An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. | No exceptions noted. |
| | | The company uses firewalls and configures them to prevent unauthorized access. | Inspected the network diagram and firewall rule sets for the production environment to determine that a firewall was in place to prevent unauthorized access. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company's formal policies outline the requirements for the following functions related to IT / Engineering:<br>• Vulnerability management<br>• System monitoring | Inspected the incident response policies and procedures to determine that formal policies outlined the requirements for the following functions related to IT / Engineering:<br>• Vulnerability management<br>• System monitoring | No exceptions noted. |
| | | Host-based vulnerability scans are performed on a continuous basis on all external-facing systems and critical and high vulnerabilities are tracked to remediation. | Inspected the operations security policy and a sample of completed vulnerability scan results and associated remediation tickets to determine that host-based vulnerability scans were performed on a continuous basis on all external-facing systems and critical and high vulnerabilities were tracked to remediation. | 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. | Data entry points are secured. | Inspected code repository configurations to determine that code repository software was in place to ensure only authorized changes were deployed into the production environment. | No exceptions noted. |
| | | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected code repository configurations and an example alert generated from the code repository to determine that the code repository software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Alerts are sent to appropriate personnel who have the authority to react to the alert. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity, and alerts were sent to appropriate personnel who have the authority to react to the alert. | No exceptions noted. |
| | | The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. | Inspected the centralized antivirus software dashboard console and the centralized antivirus configurations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configured to be updated routinely, logged, and installed on all relevant systems. | No exceptions noted. |
| | | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected the incident response plan to determine that security and privacy incident response policies and procedures were documented and communicated to authorized users. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |
| | | The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. | Inspected the network, application, database, and VPN audit logging configurations and an example audit log extract to determine that the company utilized a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. | No exceptions noted. |
| | | An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company uses firewalls and configures them to prevent unauthorized access. | Inspected the network diagram and firewall rule sets for the production environment to determine that a firewall was in place to prevent unauthorized access. | No exceptions noted. |
| | | The company's formal policies outline the requirements for the following functions related to IT / Engineering:<br>• Vulnerability management<br>• System monitoring | Inspected the incident response policies and procedures to determine that formal policies outlined the requirements for the following functions related to IT / Engineering:<br>• Vulnerability management<br>• System monitoring | 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. | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected the incident response plan to determine that security and privacy incident response policies and procedures were documented and communicated to authorized users. | No exceptions noted. |
| | | The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | Inspected the incident response plan and the supporting incident report for a sample of incidents to determine that security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC7.4 | The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. | Inspected the incident response plan to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented. | No exceptions noted. |
| | | The company tests their incident response plan at least annually. | Inspected the incident response plan and the completed tabletop exercise test results to determine that the company tested their incident response plan at least annually. | No exceptions noted. |
| | | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected the incident response plan to determine that security and privacy incident response policies and procedures were documented and communicated to authorized users. | No exceptions noted. |
| | | The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | Inspected the incident response plan and the supporting incident report for a sample of incidents to determine that security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | Inspected the business continuity and disaster recovery policy to determine that business continuity and disaster recovery plans were documented that outlined communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | No exceptions noted. |
| | | The company has a documented BC/DR plan and tests it annually. | Inspected the business continuity and disaster recovery policy and the completed tabletop exercise test results to determine that BC/DR plans were documented and tested annually. | No exceptions noted. |
| | | The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected the change management and secure development policies and procedures to determine that the company had a formal SDLC methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | | The company's data backup policy documents requirements for backup and recovery of customer data. | Inspected the data management and retention policies and procedures and an example backup log to determine that backup policies and procedures were implemented for backup and recovery of customer data. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company tests their incident response plan at least annually. | Inspected the incident response plan and the completed tabletop exercise test results to determine that the company tested their incident response plan at least annually. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Change Management** | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Data entry points are secured. | Inspected code repository configurations to determine that code repository software was in place to ensure only authorized changes were deployed into the production environment. | No exceptions noted. |
| | | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected code repository configurations and an example alert generated from the code repository to determine that the code repository software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |
| | | Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. | Inspected the code repository configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed. | No exceptions noted. |
| | | Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. | Inspected the change management and secure development policy and the supporting change ticket for a sample of system changes, infrastructure changes, and application changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impaired system operation. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Change Management** | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected the change management and secure development policy and the supporting change ticket for a sample of system changes, infrastructure changes, and application changes to determine that software and infrastructure changes were required to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | | The company restricts access to migrate changes to production to authorized personnel. | Inquired of the IT Manager regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| | | | Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized personnel. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Change Management** | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected the change management and secure development policies and procedures to determine that the company had a formal SDLC methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | | The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments. | Inspected the network segregation diagram and data management policies and procedures to determine that the company prohibited confidential or sensitive customer data, by policy, from being used or stored in non-production environments. | No exceptions noted. |
| | | The company communicates system changes to authorized internal users. | Inspected internal communication channel and the entity's website to determine that the company communicates system changes to authorized internal users. | No exceptions noted. |
| | | The company notifies customers of critical system changes that may affect their processing. | Inspected the entity's website and an example e-mail notification to determine that the company notifies customers of critical system changes that may affect their processing. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | The annual comprehensive risk assessment results are reviewed and approved by management. | Inspected the security risk management program and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by management. | No exceptions noted. |
| | | The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions. | Inspected the cybersecurity insurance documentation to determine that the company maintained cybersecurity insurance to mitigate the financial impact of business disruptions. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the security risk management program to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Inspected the third-party risk management policy and the executed third-party agreements for a sample of third-parties to determine that the company had written agreements in place with vendors and related third-parties, and these agreements included confidentiality and privacy commitments applicable to that entity. | No exceptions noted. |
| | | The company has a vendor management program in place. Components of this program include:<br>• Critical third-party vendor inventory<br>• Vendor's security and privacy requirements<br>• Review of critical third-party vendors at least annually | Inspected the third-party risk management policy, vendor inventory listing, and vendor security reviews for a sample of third-party vendors to determine that the program included requirements for:<br>• Third-party inventory<br>• Vendor's security and privacy requirements<br>• Review of third-party vendors at least annually | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| A1.1 | The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Alerts are sent to appropriate personnel who have the authority to react to the alert. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity, and alerts were sent to appropriate personnel who have the authority to react to the alert. | No exceptions noted. |
| | | The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand. | Inspected the monitoring tool configurations and the supporting change ticket for an example change made to a system as a result of a capacity constraint/issue to determine that the company evaluated system capacity on an ongoing basis and system changes were implemented to help ensure that processing capacity can meet demand. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected the change management and secure development policy and the supporting change ticket for a sample of system changes, infrastructure changes, and application changes to determine that software and infrastructure changes were required to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | | The company uses an intrusion prevention system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected the network diagram and the IPS configurations to determine that an intrusion prevention system was in place to provide continuous monitoring of the company's network and early detection of potential security breaches. | No exceptions noted. |
| | | An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Inspected the monitoring tool configurations, the antivirus software dashboard and configurations, the code repository configurations, the IPS configurations, the firewall rule sets, and the antivirus, code repository, and IPS alert configurations and an example alert to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| A1.2 | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. | Inquired of the Risk Program Manager regarding failed backup jobs to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure. | No exceptions noted. |
| | | | Inspected the data management and retention policies and procedures to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure. | No exceptions noted. |
| | | | Inspected backup configurations and an example failed backup alert to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure. | Testing of the control activity disclosed that there were no failed backups during the review period. |
| | | The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails. | Inspected the backup replication configurations and an example backup replication completion log to determine that the company's databases were replicated to a secondary data center on a real-time basis, and alerts were configured to notify administrators if replication failed. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | Inspected the business continuity and disaster recovery policy to determine that business continuity and disaster recovery plans were documented that outlined communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | No exceptions noted. |
| | | The company performs periodic backups for production data. Data is backed up to a different location than the production system. | Inspected the backup schedule and configurations and an example backup log to determine that the company performed daily backups for production data, and data was backed up to a different location than the production system. | No exceptions noted. |
| | | The company's data backup policy documents requirements for backup and recovery of customer data. | Inspected the data management and retention policies and procedures and an example backup log to determine that backup policies and procedures were implemented for backup and recovery of customer data. | No exceptions noted. |
| | | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the completed risk assessment to determine that the company performed a risk assessment on at least an annual basis, and as part of this process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed and included a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |
| A1.3 | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | Inspected the business continuity and disaster recovery policy to determine that business continuity and disaster recovery plans were documented that outlined communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | No exceptions noted. |
| | | The company has a documented BC/DR plan and tests it annually. | Inspected the business continuity and disaster recovery policy and the completed tabletop exercise test results to determine that BC/DR plans were documented and tested annually. | No exceptions noted. |
| | | The company's data backup policy documents requirements for backup and recovery of customer data. | Inspected the data management and retention policies and procedures and an example backup log to determine that backup policies and procedures were implemented for backup and recovery of customer data. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY | | | | |
|---|---|---|---|---|
| **C1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| C1.1 | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | Inspected the data management and retention policies and procedures to determine that policies and procedures were in place to guide the secure retention and disposal of company and customer data. | No exceptions noted. |
| | | The company maintains a formal inventory of production system assets. | Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets. | No exceptions noted. |
| | | The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments. | Inspected the network segregation diagram and data management policies and procedures to determine that the company prohibited confidential or sensitive customer data, by policy, from being used or stored in non-production environments. | No exceptions noted. |
| | | The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected the data management and retention policies and procedures to determine that a data classification policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel. | No exceptions noted. |
| | | The company restricts privileged access to databases to authorized users with a business need. | Inquired of the IT Manager regarding access to stored data to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY | | | | |
|---|---|---|---|---|
| **C1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the database user listing, admin listing, and access rights to determine that privileged access to databases was restricted to authorized users with a business need. | No exceptions noted. |
| | | The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Inspected the third-party risk management policy and the executed third-party agreements for a sample of third-parties to determine that the company had written agreements in place with vendors and related third-parties, and these agreements included confidentiality and privacy commitments applicable to that entity. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |
| C1.2 | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. | Inspected the data management and retention policy and the destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that the company had electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY | | | | |
|---|---|---|---|---|
| **C1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | Inspected the data management and retention policies and procedures to determine that policies and procedures were in place to guide the secure retention and disposal of company and customer data. | No exceptions noted. |

# SECTION 5

# OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

## MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results | Management's Response |
|---|---|---|---|---|
| CC1.4, CC2.2 | The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Inspected the training completion logs for a sample of new hires to determine that employees were required to complete security awareness training within thirty days of hire. | Testing of the control activity disclosed that security awareness training was not completed within thirty days of hire for 1 of 10 new hires sampled. Subsequent testing of the control activity disclosed that security awareness training was completed after 30 days of hire. | The company acknowledges the exception noted. Of the ten new hires sampled, one employee did not complete required security awareness training within thirty days of hire in accordance with company policy. The training was subsequently completed shortly after the 30-day requirement.<br><br>Upon review, the company determined this was an isolated instance resulting from an oversight in the onboarding tracking process. Management has reinforced internal onboarding procedures and reminder mechanisms to ensure training completion within the required timeframe. The company does not believe this exception represents a systemic issue or a failure in the design of the control. |