Replicon, Inc.
Type 2 SOC 2
2021

REPLICON™ The Time Intelligence™ Company

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

REPORT ON REPLICON, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

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

October 1, 2020 to September 30, 2021

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

Table of Contents

SECTION 1

ASSERTION OF REPLICON, INC. MANAGEMENT

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

REPLICON The Time Intelligence Company

ASSERTION OF REPLICON, INC. MANAGEMENT

November 9, 2021

We have prepared the accompanying description of Replicon, Inc.'s ('Replicon' or 'the Company') Replicon Cloud Platform Services System titled "Replicon, Inc.'s Description of Its Replicon Cloud Platform Services System throughout the period October 1, 2020 to September 30, 2021" (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 Replicon Cloud Platform Services System that may be useful when assessing the risks arising from interactions with Replicon's system, particularly information about system controls that Replicon 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 (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*).

Replicon uses Amazon Web Services ('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 Replicon, to achieve Replicon's service commitments and system requirements based on the applicable trust services criteria. The description presents Replicon's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Replicon's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. the description presents Replicon's Replicon Cloud Platform Services System that was designed and implemented throughout the period October 1, 2020 to September 30, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Replicon's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Replicon's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Replicon's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Replicon's controls operated effectively throughout that period.

_____
Neal Alberda
Vice President, Information Systems and Technology
Replicon, Inc.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Replicon, Inc.

Scope

We have examined Replicon's accompanying description of its Replicon Cloud Platform Services System titled "Replicon, Inc.'s Description of Its Replicon Cloud Platform Services System throughout the period October 1, 2020 to September 30, 2021" (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 October 1, 2020 to September 30, 2021, to provide reasonable assurance that Replicon's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Replicon 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 Replicon, to achieve Replicon's service commitments and system requirements based on the applicable trust services criteria. The description presents Replicon's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Replicon's 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 Replicon, to achieve Replicon's service commitments and system requirements based on the applicable trust services criteria. The description presents Replicon's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Replicon's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Replicon 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 Replicon's service commitments and system requirements were achieved. Replicon has provided the accompanying assertion titled "Assertion of Replicon, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Replicon 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.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

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.

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 Replicon's Replicon Cloud Platform Services System that was designed and implemented throughout the period October 1, 2020 to September 30, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Replicon's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Replicon's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that Replicon's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Replicon's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4*,* is intended solely for the information and use of Replicon, user entities of Replicon's Replicon Cloud Platform Services System during some or all of the period October 1, 2020 to September 30, 2021, business partners of Replicon subject to risks arising from interactions with the Replicon Cloud Platform Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, the subservice organization, 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
November 9, 2021

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

SECTION 3

REPLICON, INC.'S DESCRIPTION OF ITS REPLICON CLOUD PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2020 TO SEPTEMBER 30, 2021

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

OVERVIEW OF OPERATIONS

Company Background

Replicon was founded in 1996 and provides time tracking solutions for corporations. Replicon has over 1.5 million users from approximately 7,300 companies in 70 countries that utilize Replicon's time and expense tracking product suite to track time and expenses to manage projects, bill clients, and automate time and attendance policies within one end-to-end solution.

Replicon is a privately held company with head office operations based in Calgary, Alberta, and additional offices located in Toronto, Ontario, Redwood City, California, Bangalore, India, London, England, and Sydney, Australia. The company currently employs approximately 700 people.

Description of Services Provided

Replicon's Client Billing, Project Costing, Time and Attendance, TimeOff, Cloud Clock, WebExpense, Polaris PSA, Polaris PPM, and mobile products form the Replicon Cloud Platform Services System (Gen 3) that can be deployed individually, or as an integrated suite. Through a transparent implementation, clients do not have to maintain the product. This enables organizations to manage individual time at the department or corporate level. Whether it is one or the entire product suite, the Replicon Cloud Platform Services System allows for the client to configure the application as desired for their business needs.

Users can configure how the system works for their business requirements such as timesheet periods, preferred e-mail notifications, and timesheet format. Users can also configure authentication settings, password parameters, and other settings such as specifying an automatic idle session timeout, using a secure browser connection, or enabling hierarchy filtering. These preferences are applied to the entire system as opposed to specific individuals or particular groups of users. Some of the password security settings include alphanumeric requirements, additional special characters, minimum password length, and password expiration intervals.

The Replicon Cloud Platform Services System includes hosting the software product and related data allowing the client to access the system through the Internet 24 hours per day. Replicon's on-site and remote backup operations are designed to ensure the continuity and availability of the Replicon Cloud Platform Services System and production data.

The Replicon Cloud Platform Services System is built with high availability systems and network devices on secured and redundant infrastructure. This Software-as-a-Service (SaaS) solution runs on servers hosted within AWS across four regions, six availability zones, and two additional regions for disaster recovery.

The Replicon Cloud Platform Services System feature enhancements and defects are performed under quality control procedures in accordance with Replicon's change management process to help ensure system availability and client satisfaction.

Replicon allows users to create highly customized reports to assist with tracking and managing time, expenses, projects, and users. Reports can be viewed within the application or saved to a portable document format (PDF) or spreadsheet (CSV) document. Additionally, reports can be sent via e-mail according to predefined schedules. The reporting feature offers a wide number of options for report configuration including the following:

- Fields and filters
- Data grouping and sorting
- Indicating whether summaries should be generated

Users can also add a new report based on available report templates. Once a report exists, it can be edited. These reports can be created as either public or private reports. Public reports are available to those users assigned permission in which the report is enabled, whereas private reports are only available to the user who created them.

The Replicon Cloud Platform Services System environment is an information technology general control (ITGC) system, and user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them. Additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within the Replicon Cloud Platform Services System. This includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

Principal Service Commitments and System Requirements

Replicon designs its processes and procedures related to Replicon Cloud Platform Services System to meet its objectives for its Time Intelligence software services. Those objectives are based on the service commitments that Replicon makes to user entities, the laws and regulations that govern the provision of Time Intelligence software services, and the financial, operational, and compliance requirements that Replicon has established for the services. The Time Intelligence software services of Replicon are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Replicon operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security concepts within the fundamental designs of the Replicon Cloud Platform Services System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Use of encryption technologies to protect customer data both at rest and in transit.

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

Components of the System

Infrastructure

The primary infrastructure used to provide the Replicon Cloud Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Hosting Provider	AWS	The Replicon Cloud Platform Services System is hosted and managed by AWS
Firewall	AWS Security Groups	Controls traffic flow between servers on the internal network and between the internal network and the Internet
Storage	AWS S3	Stores information securely for longer retention

Software

The primary software used to provide the Replicon Cloud Platform Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Cloud Platform (Gen 3) system	Replicon's time and expense tracking product suite	Cloud Platform (Gen 3) system

People

Replicon has a staff of approximately 700 employees organized in the following functional areas:

- *Corporate*. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the Replicon Cloud Platform Services System primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Replicon's user entities
- *Operations*. Staff that administers the scheduling and administration of transportation providers and riders. They provide direct day-to-day services, such as transportation reservation intake, trip distribution to transportation providers, quality assurance monitoring, medical facility support, service claims adjudication, transportation network support, and reporting:
    - Customer service representatives take phone calls directly from riders to arrange transportation. These requests are entered into the Replicon Cloud Platform Services System and initiate the life cycle of a trip
    - Transportation coordinators use the Replicon Cloud Platform Services System to assign trips to transportation providers. They also manage to reroute and distribute work from the Replicon Cloud Platform Services System to the transportation providers on daily trip lists via fax. Transportation managers maintain the transportation provider network database, including updates for training, violations, screenings, and other compliance measures
    - Quality assurance (or utilization review) employees use reports generated by the Replicon Cloud Platform Services System to select samples of trips that are tested for contractual compliance and to monitor for fraud and abuse. They also take complaints from riders, facilities, and transportation providers and work to resolve them, using tools within the Replicon Cloud Platform Services System

  - The facility staff manages the facility database for the Replicon Cloud Platform Services System. They also maintain the transportation standing orders within the system and take single trip requests from facilities only
  - The claims staff receives requests for payment and adjudicates these claims in the software. This includes invoice management, trip verification, and billing support
  - A reports manager typically uses the Replicon Cloud Platform Services System to produce contract-level specific reports for Replicon's user entities
- *IT.* Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom:
  - The help desk group provides technical assistance to the Replicon Cloud Platform Services System users
  - The infrastructure, networking, and systems administration staff typically have no direct use of the Replicon Cloud Platform Services System. Rather, it supports Replicon's IT infrastructure, which is used by the software. A systems administrator deploys the releases of the Replicon Cloud Platform Services System and other software into the production environment
  - The software development staff develops and maintains the custom software for Replicon. This includes the Replicon Cloud Platform Services System, supporting utilities, and the external websites that interact with the Replicon Cloud Platform Services System. The staff includes software developers, database administration, software quality assurance, and technical writers
  - The information security staff supports the Replicon Cloud Platform Services System indirectly by monitoring internal and external security threats and maintaining current antivirus software
  - The information security staff maintains the inventory of IT assets
  - IT operations manage the user interfaces for the Replicon Cloud Platform Services System. This includes processing user entity-supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on)
  - Telecom personnel maintain the voice communications environment, provide user support to Replicon, and resolve communication problems. This group does not directly use the Replicon Cloud Platform Services System, but it provides infrastructure support as well as disaster recovery assistance

Data

Data, as defined by Replicon, constitutes the following:

- Master transportation file data
- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Transaction processing is initiated by the receipt of a trip or standing order request. This request typically comes directly from a rider or treating facility by telephone or via the websites, or it may arrive by fax from a treating facility. After the trip is completed, the transportation provider sends Replicon paper documents with daily trip information, including information about completed trips, cancellations or no-shows, and weekly driver logs, which is entered into the system's verification module; a portion of this trip completion information may be entered on the Replicon transportation provider web interface.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from various websites. The availability of these reports is limited by job function. Reports delivered externally are sent using a secure method-encrypted e-mail, secure file transfer protocol (FTP), or secure websites-to transportation providers, treating facilities, and governments or managed care providers using Replicon-developed websites or over connections secured by trusted security certificates. Replicon uses Transport Layer Security (TLS) to encrypt e-mail exchanges with government or managed care providers, facility providers, and transportation providers.

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 Replicon policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Replicon team member.

Physical Security

The in-scope system and supporting infrastructure are hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

Logical Access

Replicon 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, Replicon 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.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Replicon network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user 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.

Employees accessing the system from outside the Replicon network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Replicon network.

Customer employees' access the Replicon Cloud Platform Services System through the Internet using the SSL functionality of their web browser. These customer employees supply a valid user ID and password to gain access to customer cloud resources. Passwords conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Replicon's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a daily basis. This daily report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete access roles from IDs belonging to terminated employees.

On a quarterly 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 CISO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

Replicon protects business-critical information from loss or corruption. Backups or duplication of the information is a mitigating factor to the risk of availability and integrity of information. Backup or replication processes should be implemented per the business and customer needs and service level agreements.

Replicon implements a backup plan for accurate and complete backup and restoration procedures. The plan defines the extent (i.e., full vs. differential backups) and frequency of backups to reflect Replicon's business and security requirements, as well as the criticality of the information to the continued operation of the business.

Backup copies should be stored in a secured location so it can be retrieved should the original information become unavailable.

Backups should be tested annually, in conjunction with the restoration procedures, to ensure backups are in good working order should restoration be required.

Operational procedures should monitor backup execution and address failures with scheduled backups to ensure completeness of the process.

Computer Operations - Availability

Replicon maintains policies and procedures to guide cloud operations personnel in data backup and replication processes. Replicon utilizes AWS' S3 to manage and maintain the production data supporting the Replicon Cloud Platform Services System. Data stored within AWS S3 includes cross-region replication which automatically replicates the data across different AWS regions. The data processed using AWS' EC2 is stored in RDS databases that are backed up on a daily basis (AWS S3 refers to daily full backups as snapshots).

AWS has built-in redundancies for the snapshot/backup data as the data is deployed using availability zones. If one availability zone were to fail, AWS has built-in redundancy to another zone within the same or different region. Therefore, snapshot/backup data is maintained separately from production.

As part of normal cloud operations, cloud operations personnel perform restores of production data on a monthly basis, and the AWS system maintains an inventory of backup data for restoration purposes. The ability to access backup and replicated data within AWS is restricted to authorized members of the cloud operations team.

Cloud operations personnel maintain policies and procedures to guide personnel in performing AWS instance builds, patch management, and incident management in the production environment. The production network is configured with failover processes and redundant architecture that is inherent within the AWS management console to mitigate the risk of disruption of business operations.

An environmental monitoring system is in place to monitor the availability and performance of the production servers and network devices. The system is configured to send automated e-mail alerts to cloud operations personnel when pre-defined thresholds are exceeded. Upon receipt of an alert, cloud operations personnel investigate the issue and determine what actions are required to resolve the issue.

Change Control

Replicon 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 to developers.

Replicon has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches. Customers and Replicon system owners review proposed operating system patches to determine whether the patches are applied. Customers and Replicon systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Replicon staff validates that patches have been installed and if applicable, that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Replicon. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on an annual basis. The third-party vendor uses industry-standard scanning technologies and a formal methodology specified by Replicon. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Replicon system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Replicon cloud operations personnel follow the AWS "best practices" guide to provide a network security framework for their production environment. AWS EC2 security groups are in place to provide perimeter security for the Replicon Cloud Platform Services System environment. The security groups monitor incoming network traffic by analyzing the data packets and determining whether they should be allowed based on the ruleset. The ability to modify the security groups is restricted to authorized cloud operations personnel via the AWS management console. Cloud operations personnel are required to authenticate to the AWS management console using a user account, password, and multi-factor authentication code in order to perform any modifications to the security groups. The AWS management console is configured to enforce password requirements that include minimum length and password complexities.

The production systems hosted by AWS are protected from unauthorized Internet traffic. The dynamic/private Transmission Control Protocol (TCP) is the only protocol open to filter unauthorized traffic. In addition, traffic trying to authorize against the AWS management console to access Replicon's production systems is required to authenticate with a user account, password, and a multi-factor authentication code. Administrative access to the AWS console is restricted to authorized cloud operations personnel.

Boundaries of the System

The scope of this report includes the Replicon Cloud Platform Services System performed in Calgary, Alberta; Toronto, Ontario; Redwood City, California; Bangalore, India; London, England, and Sydney, Australia facilities.

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

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Replicon's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Replicon's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees to 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

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Replicon's control environment affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Replicon's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. These include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that the service organization has implemented in this area are described below:

- Organizational policy statements and codes of conduct are documented and communicated to employees
- The employee policy and procedures manual contain organizational policy statements and codes of conduct to which employees are required to adhere
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- Employees sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties

Commitment to Competence

Replicon's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

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

Replicon's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Replicon's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Replicon's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they are held accountable.

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

Replicon's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Replicon's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgment 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

Replicon's risk assessment process identifies and manages risks that could potentially affect Replicon's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Replicon identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Replicon, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Replicon has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Replicon attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Management is responsible for identifying the risks that threaten the achievement of the commitments stated in the management's description of the service organization's system. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them. However, because commitments relate to risk that controls seek to mitigate, management thoughtfully identified controls when designing, implementing, and documenting their system.

In order to identify the risk associated with each criterion, a risk level assessment is performed on the control activities found within the respective criteria. Each control activity is reviewed by management and departmental personnel to determine whether Replicon's ability to adhere to the control activity as stated exists and the probability that Replicon maintains adherence using a grading system of high, medium, and low.

Replicon's methodology for analyzing risks varies, largely because many risks are difficult to quantify. The process includes:

- Estimating the significance of a risk as it relates to the information security attributes of confidentiality, integrity, and availability
- Assessing the likelihood or frequency of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken to mitigate these risks
- Periodically identifying, analyzing, and prioritizing threats to information assets and their supporting infrastructure
- Evaluating findings from risk assessment activities and integrating them into the security awareness and training program
- Utilizing screening procedures such as background checks for personnel and evaluations for potential third-party service providers
- Establishing and tracking representative metrics for gauging progress
- Developing and exercising formal plans for responding to information security intrusions and incidents
- Establishing associated metrics for gauging the effectiveness of these plans

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Replicon's Cloud Platform system; as well as the nature of the components of the system result in risks that the criteria are not met. Replicon 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 are unique. As part of the design and operation of the system, Replicon's management identifies the specific risks that the criteria are not met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Replicon's 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, information technology. At Replicon, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly 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, meetings are held annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the 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 Replicon personnel via e-mail messages.

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

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Replicon's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Replicon's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Replicon's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Replicon's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

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 in the Last 12 Months

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

Criteria Not Applicable to the System

All Common criteria were applicable to the Replicon Cloud Platform Services System.

Subservice Organizations

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

Subservice Description of Services

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

Complementary Subservice Organization Controls

Replicon's 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 Replicon's services to be solely achieved by Replicon control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish its own internal controls or procedures to complement those of Replicon.

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	Recovery key materials used for disaster recovery processes by 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 documentation.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		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.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television (CCTV) is used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

Replicon 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. In addition, Replicon performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

Replicon's 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 Replicon's services to be solely achieved by Replicon control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Replicon's.

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 configuring the Replicon Cloud Platform Services System application password parameters and complexity requirements settings.
2. User entities are responsible for administering Replicon Cloud Platform Services System security access privileges.
3. User entities are responsible for ensuring the supervision, management, and control of the use of Replicon services by their personnel.
4. User entities are responsible for removing terminated employees' access to the Replicon Cloud Platform Services System in a timely manner.
5. User entities are responsible for maintaining their own system(s) of record.
6. User entities are responsible for defining an appropriate encryption methodology utilized in relation to Replicon's systems.
7. User entities are responsible for determining whether Replicon's security infrastructure is appropriate for its needs and notifying Replicon of any requested modifications.

8. User entities are responsible for immediately notifying Replicon of any actual or suspected information security breaches, including compromised user accounts.
9. User entities are responsible for obtaining release notes from the Replicon website.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

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 Replicon's description of the system. Any applicable trust services criteria that are not addressed by control activities at Replicon 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

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:15UTC

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

A-LIGN ASSURANCE's examination of the controls of Replicon was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Replicon and did not encompass all aspects of Replicon's 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; and
- 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.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Upon hire, personnel are required to sign a non-disclosure agreement.	Inspected the signed non-disclosure agreement for a sample of new hires to determine that upon hire, personnel were required to sign a non-disclosure agreement.	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**
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check results for a sample of new hires to determine that prior to employment, personnel were required to complete a background check prior to employment.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation tracking spreadsheet for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the disciplinary policy to determine that sanction policies, which included probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the ethical reporting portal to determine that employees were directed on how to report unethical behavior in a confidential manner.	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**
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and internal controls matrix to determine that executive management-maintained independence from those that operate the key controls within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the information security management committee (ISMC) meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
			Inspected the ISMC meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	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**
		A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.	Inspected the entity's completed attestation reports to determine that a third-party performed an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.	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.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity’s job portal.	Inspected the documented job description for a sample of open job roles and the entity's job portal to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity’s job portal.	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**
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the documented job description for a sample of open job roles on the entity's job portal to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, internal controls matrix, and the documented job description for a sample of open job roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the candidate evaluation process as well as the competency and training requirements for personnel.	Inspected the new hire evaluation and training policies to determine that policies and procedures were in place that outlined the candidate evaluation process as well as the competency and training requirements for personnel.	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**
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation tracking spreadsheet for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	Inspected the interview questionnaire for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the documented job description for a sample of open job roles and interview questionnaire for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training materials to determine that executive management created a training program for its employees.	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**
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check results for a sample of new hires to determine that prior to employment, personnel were required to complete a background check prior to employment.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's job portal.	Inspected the documented job description for a sample of open job roles and the entity's job portal to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's job portal.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	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**
		Policies and procedures are in place that outline the candidate evaluation process as well as the competency and training requirements for personnel.	Inspected the new hire evaluation and training policies to determine that policies and procedures were in place that outlined the candidate evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation tracking spreadsheet for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the disciplinary policy to determine that sanction policies, which included probation, suspension and termination, were in place for employee misconduct.	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.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	Inspected the information security policies and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the IPS configurations, encryption methods and configurations and VPN authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the data classification policy to determine that data was retained for only as long as required to perform the required system functionality, service or use.	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**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's job portal.	Inspected the documented job description for a sample of open job roles and the entity's job portal to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's job portal.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's intranet.	Inspected the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the entity's intranet.	No exceptions noted.
		Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	Inspected the signed employee handbook, and training completion certificates for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	No exceptions noted.
		Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.	Inspected the signed employee handbook, and training completion certificates for a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.	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**
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Executive management meets bi-weekly with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the ISMC meeting minutes for a sample of bi-weekly security meetings to determine that executive management met bi-weekly with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the ethical reporting portal to determine that employees were directed on how to report unethical behavior in a confidential manner.	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**
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet.	Inspected the incident management policy and the entity's intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's intranet.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's company meetings.	Inspected the entity's company-wide objectives meetings to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's company meetings.	No exceptions noted.
		Employees are required to attend security awareness training annually.	Inspected the training completion certificates for a sample of current employees to determine that employees were required to attend security awareness training annually.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the security awareness training tracker to determine that management tracked and monitored compliance with information security and awareness training requirements.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Third-party agreements delineate the boundaries of the system and describe relevant system components.	Inspected the executed third-party agreement for a sample of third parties to determine that third-party agreements delineated the boundaries of the system and described relevant system components.	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**
		Third-party agreements communicate the system commitments and requirements of third parties.	Inspected the executed third-party agreement for a sample of third parties to determine that third-party agreements communicated the system commitments and requirements of third parties.	No exceptions noted.
		The information security policies and procedures that communicate the system commitments and supporting resources are provided to external users.	Inspected the entity's customer portal to determine that the information security policies and procedures that communicate the system commitments and supporting resources were provided to external users.	No exceptions noted.
		Third-party agreements outline and communicate the terms, conditions and responsibilities of third parties.	Inspected the executed third-party agreement for a sample of third parties to determine that third-party agreements outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the master services agreement template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the completed agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	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**
		Changes to commitments, requirements and responsibilities are communicated to customers via website notices.	Inspected the entity's website to determine that changes to commitments, requirements and responsibilities were communicated to customers via website notices.	No exceptions noted.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.	Inspected the master services agreement template to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and shared with external parties.	No exceptions noted.
		Executive management meets annually with operational management to discuss the results of assessments performed by third parties.	Inspected the ISMC meeting minutes to determine that executive management met annually with operational management to discuss the results of assessments performed by third parties.	No exceptions noted.
		Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the ethical reporting portal to determine that employees were directed on how to report unethical behavior in a confidential manner.	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.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk management policy to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected the completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	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**
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee new hire evaluation policy, the entity's documented objectives and strategies and the documented key performance indicators to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the entity's all hands meeting minutes and documented objectives and strategies to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls framework is based on a recognized ISO 27001 framework.	Inspected the completed compliance reports to determine that the entity's internal controls framework was based on a recognized ISO 27001 framework.	No exceptions noted.
		The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards.	Inspected the entity's completed attestation reports to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations and standards.	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.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	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 entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	Inspected the risk management policy to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	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**
			Inspected the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk management policy to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	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**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	Inspected the risk management policy to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk management policy to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	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**
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk management policy to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
			Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk management policy to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
			Inspected the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	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**
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.	Inspected the risk management policy to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third parties.	No exceptions noted.
			Inspected the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third parties.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	Inspected the completed risk assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	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**
		As part of management's assessment of fraud risks, management considers key fraud factors such as the opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as the opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk management policy to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk management policy to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	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**
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk management policy to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	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.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IPS configurations, and firewall rule sets 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.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected ISMC meeting minutes to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Logical access reviews are performed on a monthly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on a monthly basis.	No exceptions noted.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the vulnerability scan results for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	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**
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		A third-party performs an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	Inspected the entity's completed attestation reports to determine that a third-party performed an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation tracking spreadsheet for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed vendor review tracker and vendor security policy to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	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**
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
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.	Vulnerabilities, deviations and control gaps identified from the risk and compliance assessments are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the vulnerability report and solutions for a sample of months to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations and control gaps identified from the risk and compliance assessments are documented, investigated, and addressed.	Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	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 the vulnerability report and solutions for a sample of months to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
		Vulnerabilities, deviations and control gaps identified from the risk and compliance assessments are addressed by those parties responsible for taking corrective actions.	Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the vulnerability report and solutions for a sample of months to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the ISMC meeting minutes to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	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.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Inspected the completed risk and compliance assessments to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the vulnerability report and solutions for a sample of months to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	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**
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk management policy to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery policy to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	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**
		Business continuity and disaster recovery plans are tested on a monthly basis.	Inspected the completed business continuity and disaster recovery test results for a sample of months to determine that the business continuity and disaster recovery plans were tested on a monthly basis.	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.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet.	Inspected the information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to employees through the entity's intranet.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of unavailable technology processing.	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 internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what was required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	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.	Organizational and information security policies and procedures are documented and made available to employee's through the entity's intranet.	Inspected the information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to employees through the entity's intranet.	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 organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's job portal.	Inspected the documented job description for a sample of open job roles and the entity's job portal to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's job portal.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	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.	An inventory of system assets and components is maintained to classify and manage the information 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.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding administrative access to determine that network administrative access was restricted to only authorized personnel.	No exceptions noted.
			Inspected the network administrator user listing and access rights to determine that network administrative access was restricted to only authorized personnel.	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**
		Networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age • Password length • Complexity	No exceptions noted.
		Network users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Compliance Analyst login to the network to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Network account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	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**
		Network audit logging settings are in place that include: • Account logon events • Account management • Object access • Privilege use • System events	Inspected the network audit logging settings and a sample network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Object access • Privilege use • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the network audit logging settings and a sample network audit log extract to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	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**
		Operating system administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding administrative access to determine that operating system administrative access was restricted to only authorized personnel.	No exceptions noted.
			Inspected the operating system administrator user listing and access rights to determine that operating system administrative access was restricted to only authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age • Password length • Complexity	No exceptions noted.
		Operating system users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Compliance Analyst login to the operating system to determine that operating system users were authenticated via individually assigned user accounts 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**
		Operating system account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	No exceptions noted.
		Operating system audit logging settings are in place that include: • Account logon events • System events	Inspected the operating system audit logging settings and a sample operating system audit log extract to determine that operating system audit logging configurations were in place that included: • Account logon events • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the operating system audit logging settings and a sample operating system audit log extract to determine that operating system audit logs were maintained and reviewed as-needed.	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**
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding database administrative access to determine that database administrative access was restricted to only authorized personnel.	No exceptions noted.
			Inspected the database administrator user listing and access rights to determine that database administrative access was restricted to only authorized personnel.	No exceptions noted.
		Databases are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the database password settings to determine that database was configured to enforce password requirements that included: • Password history • Password age • Password length • Complexity	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**
		Database users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Compliance Analyst login to the database to determine that database users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	No exceptions noted.
		Database audit logging settings are in place that include: • Account logon events • Object access • System events	Inspected the database audit logging settings and a sample database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Object access • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that the database audit logs were maintained and reviewed as-needed.	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 audit logging settings and a sample database audit log extract to determine that database audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding application administrative access to determine that application administrative access was restricted to only authorized personnel.	No exceptions noted.
			Inspected the application administrator user listing and access rights to determine that application administrative access was restricted to only authorized personnel.	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 application is configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password age • Password length • Complexity	No exceptions noted.
		Application users are authenticated via individually assigned user accounts and passwords.	Observed the Senior Compliance Analyst login to the application to determine that application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Application account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	No exceptions noted.
		Application audit policy settings are in place.	Inspected the application audit logging settings and a sample application audit log extract to determine that application audit logging configurations were in place.	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**
		Application audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding application audit logs to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the application audit logging settings and a sample application audit log extract to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Remote Access (Okta)			
		Virtual Private Network (VPN) user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • Director of Information Technology (IT) • VP of Global IT/Information Systems (IS) • IT Technical Architect	Inquired of the Information Security and Compliance Manager regarding VPN administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel: • Director of IT • VP of Global IT/IS • IT Technical Architect	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 administrator user listing to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel: • Director of IT • VP of Global IT/ IS • IT Technical Architect	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an Intrusion Prevention System (IPS).	Inspected the IPS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IPS.	No exceptions noted.
		A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	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**
		Critical data is stored in encrypted format using Advanced Encryption Standard (AES) 256.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inspected the cryptography controls policy to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		The entity restricts access to its environment using the following mechanisms: • Classifying data • Port restrictions • Access protocol restrictions • User identification • Digital certifications	Inspected the data classification policy, listings of users with access to the network, operating system, database and application, firewall rule sets and digital certificates to determine that the entity restricted access to its environment using the following mechanisms: • Classifying data • Port restrictions • Access protocol restrictions • User identification • Digital certifications	No exceptions noted.
		Logical access reviews are performed on a monthly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on a monthly basis.	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**
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, user access listings, and supporting user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, user access listings and supporting user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, user access listings, and supporting user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	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**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, user access listings and supporting user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on a monthly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on a monthly basis.	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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, user access listings, and supporting user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	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**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, user access listings and supporting user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on a monthly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of months to determine that logical access reviews were performed on a monthly basis.	No exceptions noted.
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	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**
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	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.
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.	Policies and procedures are in place to guide personnel in data disposal and destruction.	Inspected the data retention policy and schedule to determine that policies and procedures were in place to guide personnel in data disposal and destruction.	No exceptions noted.
		The entity purges backup data, automatically, per a defined schedule.	Inspected the backup retention configurations to determine that the entity purged backup data, automatically, per a defined schedule.	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**
		Data that is no longer required for business purposes is rendered unusable.	Inquired of the Information Security and Compliance Manager regarding the data disposal process to determine that data that was no longer required for business purposes was rendered unusable.	No exceptions noted.
			Inspected the data retention policy and schedule to determine that data that was no longer required for business purposes was rendered unusable.	No exceptions noted.
			Inspected the supporting service ticket for a sample of requests to dispose of data to determine that data that was no longer required for business purposes was rendered unusable.	Testing of the control activity disclosed that there were no requests to dispose of data that occurred during the review period.
		Policies and procedures are in place for removal of media storing critical data or assets.	Inspected the asset management policy to determine that policies and procedures were in place for removal of media storing critical data or assets.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN and TLS technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN and TLS technologies were used for defined points of connectivity.	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**
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the Senior Compliance Analyst authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	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 remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Information Security and Compliance Manager regarding the ability to access stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the centralized firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	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 centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected the IPS configurations, a sample IPS log extract and a sample alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	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 centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Critical data is stored in encrypted format using AES-256.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media settings to determine that the use of removable media was prohibited by policy except when authorized by management.	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 removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	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.	Logical access to stored data is restricted to authorized personnel.	Inquired of the Information Security and Compliance Manager regarding the ability to access stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Backup media is replicated to a secondary location, on a daily basis.	Inspected the backup replication settings to determine that backup media was replicated to a secondary location, on a daily basis.	No exceptions noted.
		The ability to restore backed up data is restricted to authorized personnel.	Inquired of the Information Security and Compliance Manager regarding the ability to restore backup data to determine that the ability to restore backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the list of users with the ability to restore backup data to determine that the ability to restore backed up data was restricted to authorized personnel.	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 entity secures its environment a using multi-layered defense approach that includes firewalls, an IPS, antivirus software and bastion hosts.	Inspected the network diagram, IPS configurations, firewall rule sets, antivirus settings and DMZ settings to determine that the entity secured its environment a using multi-layered defense approach that included firewalls, an IPS, antivirus software and bastion hosts.	No exceptions noted.
		VPN and TLS technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN and TLS technologies were used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the Senior Compliance Analyst authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	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 remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the centralized firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	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**
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected the IPS configurations, a sample IPS log extract and a sample alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		Critical data is stored in encrypted format using AES-256.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the centralized encryption configurations for company mobile devices to determine that mobile devices were protected through the use of secured, encrypted connections.	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**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media settings to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Accessing the entity's environment from a mobile device requires a valid user ID and password.	Observed the Senior Compliance Analyst access the entity's environment from a mobile device to determine that accessing the entity's environment from a mobile device required a valid user ID and password.	No exceptions noted.
			Inspected the endpoint management tool configurations to determine that accessing the entity's environment from a mobile device required a valid user ID and password.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Information Security and Compliance Manager regarding the ability to implement changes to production 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 and appropriate users.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	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 antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.	Inspected the vulnerability management policy to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment.	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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IPS configurations, and firewall rule sets 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.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, the IPS configurations and a sample IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	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 IPS is configured to notify personnel upon intrusion prevention.	Inspected the IPS configurations, a sample IPS log extract and a sample alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media settings to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the centralized firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	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**
			Inspected the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the vulnerability scan results for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	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**
CC7.2	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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management policy to determine documented that incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, the IPS configurations and a sample IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	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.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IPS configurations, and firewall rule sets 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.	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**
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected the IPS configurations, a sample IPS log extract and a sample alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the centralized firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	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 firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the centralized antivirus configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	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 antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media settings to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
	Network			
		Network account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	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**
		Network audit logging settings are in place that include: • Account logon events • Account management • Object access • Privilege use • System events	Inspected the network audit logging settings and a sample network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Object access • Privilege use • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the network audit logging settings and a sample network audit log extract to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	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**
		Operating system audit logging settings are in place that include: • Account logon events • System events	Inspected the operating system audit logging settings and a sample operating system audit log extract to determine that operating system audit logging configurations were in place that included: • Account logon events • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the operating system audit logging settings and a sample operating system audit log extract to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Database			
		Database account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	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**
		Database audit logging settings are in place that include: • Account logon events • Object access • System events	Inspected the database audit logging settings and a sample database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Object access • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that the database audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the database audit logging settings and a sample database audit log extract to determine that database audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Application			
		Application account lockout settings are in place that include: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout threshold • Account recovery e-mail • Account password recovery questions complexity	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**
		Application audit policy settings are in place.	Inspected the application audit logging settings and a sample application audit log extract to determine that application audit logging configurations were in place.	No exceptions noted.
		Application audit logs are maintained and reviewed as-needed.	Inquired of the Information Security and Compliance Manager regarding application audit logs to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the application audit logging settings and a sample application audit log extract to determine that application audit logs were maintained and reviewed as-needed.	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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management policy to determine documented that incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident management policy to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	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 incident management policy defines the classification of incidents based on its severity.	Inspected the incident management policy to determine that the incident management policy defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident management policy to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	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**
			Inspected the incident management policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the incident management policy to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.

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**
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the incident management policy to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.

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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management policy to determine documented that incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident management policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.

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 actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the incident management policy to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident management policy to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that resolution of incidents was documented within the ticket and communicated to affected 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**
			Inspected the incident management policy to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident management policy to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.

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**
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Information Security and Compliance Manager regarding the incident management process to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the incident management policy to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that there were no incidents that occurred during the review period.

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.	System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policy to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies, and the system build guides for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Backup restoration tests are performed on a monthly basis.	Inspected the completed backup restoration test results for a sample of months to determine that backup restoration tests were performed on a monthly basis.	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**
		A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery policy to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on a monthly basis.	Inspected the completed business continuity and disaster recovery test results for a sample of months to determine that the business continuity and disaster recovery plans were tested on a monthly basis.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery policy and completed business continuity and disaster recovery test results for a sample of months to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	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.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests- Development / Engineering, Site Reliability Engineering (SRE) and / or Product Management teams • Development- Engineering/Development team • Testing-quality assurance department • Implementation-Cloud Operations team	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests- Development / Engineering, SRE and / or Product Management teams • Development- Engineering / Development team • Testing-quality assurance department • Implementation-Cloud Operations Team	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the supporting ticket for a sample of application and infrastructure changes to determine that system changes were communicated to both affected internal and external users.	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**
			Inspected the marketing newsletters for a sample of weeks to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Information Security and Compliance Manager regarding access to implement changes to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
			Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting ticket for a sample of application and infrastructure changes to determine that system changes were authorized and approved by management prior to implementation.	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 change control repository dashboard 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.

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**
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting ticket for a sample of application and infrastructure changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting ticket for a sample of application and infrastructure changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
		System changes implemented to the production environment are evaluated for impact to the entity's objectives.	Inspected the supporting ticket for a sample of application and infrastructure changes to determine that system changes implemented to the production environment were evaluated for impact to the entity's objectives.	No exceptions noted.
		System changes implemented for remediating incidents follow the standard change management process.	Inquired of the Information Security Compliance Manager regarding the change management process to determine that system changes implemented for remediating incidents followed the standard change management process.	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**
			Inspected the change management policy to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policy to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	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.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk management policy to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	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**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	Inspected the risk management policy to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk • Exclude the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk management policy to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	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 entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance policy documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor security policy to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor security policy to determine that management developed third-party risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment and vendor review tracker to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor security policy to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	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**
			Inspected the completed risk assessment and vendor review tracker to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Third-party agreements outline and communicate: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	Inspected the executed third-party agreement for a sample of third parties to determine that third-party agreements outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed risk assessment and vendor review tracker to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	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**
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the vendor security policy to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.