ACD Direct
Type 2 SOC 2
2021

REPORT ON ACD DIRECT'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

July 1, 2020 to August 31, 2021

Table of Contents

SECTION 1

ASSERTION OF ACD DIRECT MANAGEMENT

ASSERTION OF ACD DIRECT MANAGEMENT

September 30, 2021

We have prepared the accompanying description of ACD Direct's ('ACD' or 'the Company') Non-Profit Marketing and Pledge Call Center Services System titled "ACD Direct's Description of Its Non-Profit Marketing and Pledge Call Center Services System throughout the period July 1, 2020 to August 31, 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 Non-Profit Marketing and Pledge Call Center Services System that may be useful when assessing the risks arising from interactions with ACD's system, particularly information about system controls that ACD 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*).

ACD uses Flexential ('subservice organization') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ACD, to achieve ACD's service commitments and system requirements based on the applicable trust services criteria. The description presents ACD's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ACD'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 ACD, to achieve ACD's service commitments and system requirements based on the applicable trust services criteria. The description presents ACD's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ACD's controls.

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

a. the description presents ACD's Non-Profit Marketing and Pledge Call Center Services System that was designed and implemented throughout the period July 1, 2020 to August 31, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2020 to August 31, 2021, to provide reasonable assurance that ACD'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 ACD's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2020 to August 31, 2021, to provide reasonable assurance that ACD'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 ACD's controls operated effectively throughout that period.

William Davis

William Davis
Director of IT Engineering
ACD Direct

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ACD Direct

Scope

We have examined ACD's accompanying description of its Non-Profit Marketing and Pledge Call Center Services System titled "ACD Direct's Description of Its Non-Profit Marketing and Pledge Call Center Services System throughout the period July 1, 2020 to August 31, 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 July 1, 2020 to August 31, 2021, to provide reasonable assurance that ACD'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*).

ACD uses Flexential to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ACD, to achieve ACD's service commitments and system requirements based on the applicable trust services criteria. The description presents ACD's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ACD'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 ACD, to achieve ACD's service commitments and system requirements based on the applicable trust services criteria. The description presents ACD's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ACD'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

ACD 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 ACD's service commitments and system requirements were achieved. ACD has provided the accompanying assertion titled "Assertion of ACD Direct Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ACD is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

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

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

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 ACD's Non-Profit Marketing and Pledge Call Center Services System that was designed and implemented throughout the period July 1, 2020 to August 31, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2020 to August 31, 2021, to provide reasonable assurance that ACD'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 ACD's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2020 to August 31, 2021, to provide reasonable assurance that ACD'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 ACD'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 ACD, user entities of ACD's Non-Profit Marketing and Pledge Call Center Services System during some or all of the period July 1, 2020 to August 31, 2021, business partners of ACD subject to risks arising from interactions with the Non-Profit Marketing and Pledge Call Center Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
September 30, 2021

SECTION 3

ACD DIRECT'S DESCRIPTION OF ITS NON-PROFIT MARKETING AND PLEDGE CALL CENTER SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2020 TO AUGUST 31, 2021

OVERVIEW OF OPERATIONS

Company Background

ACD was founded as a contact center service provider and utilized their partnerships and the exposure to coast-to-coast markets to provide viable solutions, best practices, and guidance when and where needed.

Experienced: Since 2003, ACD has been a virtual business continually working to expand their solutions and partnerships with public entities and nonprofit organizations across the United States, while adhering to the core values of being people-centric, proactive and a solutions broker. ACD currently provides customized solutions to more than 200 clients, the majority being public media stations.

Qualified: ACD strives to gain in-depth insight into their client's industry and to understand the needs, demands and challenges. ACD takes the time to collaborate with experienced vendors and industry experts to help align with the goals and objectives of each client.

Responsive: ACD provides 24/7 support to everyone involved from the client and its constituents to their agents. ACD responds by providing inbound and outbound call services, web-based support options (chat, text, e-mail) and applications to facilitate customer information management.

Description of Services Provided

ACD provides Database Management Solution services with advanced communications throughout the United States. The Company was founded in 2003 to provide Non-Profit Marketing and Pledge Center Services System to its customers. ACD's integration of a database management solution with an advanced communications platform helps automate and optimize communications.

Description of Services:

- Outbound and Inbound Call Services
- Web Based Chat Support
- Click to Dial - The "Click to Chat" option allows visitors on the customer's website to be quickly connected to one of ACD's agents
- Text Messaging/E-mail Support
- Tiered Member Services Support - Member Services Support ('MSS') provides customers with scalable support. This skill-based tiering allows customers to choose the level of support necessary from solving coverage issues
- Custom Development Team - ACD's development team can create a customizable solution to meet customer's specific needs
- SimpleScript - SimpleScript is a dynamic and fully customizable scripting solution for call handling needs. All payment processing is handled through third-party application programming interface ('API'). Data captured within SimpleScript can be exported in a wide variety of formats via several secure transmission vehicles. (i.e., Web Service, File Transfer Protocol ('FTP'), Direct Download)
- Ticketing-Based Help Desk Application - Issue tracking is handled through ACD's Help Desk Application
- Trouble Shooter - ACD's Trouble shooter is built on a foundation of decision tree scripting. Quick answers to common questions allow a call path to be handled efficiently. Additional options can be added at any time
- Referral Database Warehousing - SimpleScript is ACD's Referral Database module which streamlines information storage by housing lists of contacts in a searchable, easily accessible format. Information will be at the ready when needed
- MC 2.0 and PledgeCart 3.0 - Capture data from anywhere or anytime. These applications were built on the same premise of SimpleScript
- Payment Processing Integration - ACD has integrated with several major payment processing gateways. ACD is Level 1 Payment Card Industry ('PCI') Compliant

- Reporting Suite - ACD's reporting suite allows customers the ability to track calls and transactions with ease. Reports can be accessed from anywhere allowing customers to gauge the success of their campaign 24/7/365
- On Hold Streaming - On Hold Streaming is a service offered that provides callers with relevant content with the power of live streaming. This is optimized for the telecommunications medium to ensure that callers have the best listening experience
- Call-Center-In-A-Box Total.Care Solution - This is a web-based platform that plays the role of switchboard, receptionist, and answering service, allowing customers to manage and route all phone calls, set users/voice-mails/greetings, and streamline communications
- Cloud Based Telephony Platform - By utilizing a cloud base telephony platform, ACD can offer a highly flexible, customized contact routing solution that supports call routing and web-based chat support. Cloud based routing is secure and provides necessary redundancy to limit outages
- Toll Free/Local Number Procurement Assistance - ACD can help with procuring toll free or local numbers (i.e., Vanity Number). ACD can also assist with customers' search and purchase of this number

Donations are tracked through the payment cycle, from initial call assignment to completion of the payment. System-generated reports provide supporting documentation for donations.

Information is shared with user entities by telephone, FTP, e-mail, Electronic Data Exchange ('EDI'), and secured websites.

Principal Service Commitments and System Requirements

ACD designs its processes and procedures related to Non-Profit Marketing and Pledge Center Services System to meet its objectives for its marketing and pledge call services. Those objectives are based on the service commitments that ACD makes to user entities, the laws and regulations that govern the provision of marketing and pledge call services, and the financial, operational, and compliance requirements that ACD has established for the services. The marketing and pledge call services of ACD 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 ACD operates.

To safeguard ACD's information technology resources and to protect the confidentiality of data, adequate security measures must be taken. ACD's Full Security Policy reflects ACD's commitment to comply with required standards governing the security of sensitive and confidential information.

ACD minimizes inappropriate exposures of confidential or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses ACD's information technology resources. It is the responsibility of employees, contractors, business partners, and agents of ACD. Each is familiar with this policy's provisions and the importance of adhering to it when using ACD's computers, networks, data, and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the Information Technology ('IT') Supervisor and Director of IT at ACD.

All ACD employees undergo background checks and participate in annual security trainings, security scans, and performance reviews. They acknowledge all company policies through ADP, ACD's payroll processor.

All ACD clients understand and acknowledge their security and confidentiality roles related to data, as spelled out in contracts and letters of agreement.

All ACD data partners and data vendors meet or exceed the compliance levels and standards as ACD.

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 Non-Profit Marketing and Pledge Center Services System.

Components of the System

Infrastructure

Primary infrastructure used to provide ACD's Non-Profit Marketing and Pledge Call Center Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewall	PaloAlto	Filters traffic from the internet to MGMT
Firewall	PaloAlto	Filters traffic redundantly to the demilitarized zone ('DMZ') network
Switches	Cisco	Splits up network traffic between MGMT DMZ
Switches	Cisco	Splits up network traffic between MGMT local area network ('LAN')
Server Hardware	Dell ESX	1u host server MGMT
Server Hardware	Dell ESX	1u host server DMZ
Server Hardware	Dell ESX	1u host server LAN
VM's	VMware ESXi Host	Integrates ACD's ESX servers into a virtual environment
NAC	Milton	This appliance is referenced by gateway and CWW for Contact Center agents to be able to user ACD's applications. Users must comply with this device's security policies before being able to access their accounts in GW/CWW for the application

Software

Primary software used to provide ACD's Non-Profit Marketing and Pledge Call Center Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
VMware	VMware ESXi	Enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers
Kayako	Ubuntu Linux (64-bit)	Help desk support ticket software
Microsoft SQL	Microsoft Windows Server 2012 (64-bit)	Database software
AtomicOSSEC	Centos 7	Network monitoring software. Incident management

Primary Software		
Software	**Operating System**	**Purpose**
McAfee	Microsoft Windows Server 2012 (64-bit)	Antivirus Software

People

The ACD staff provides support for the above services in each of the following functional areas:

- Executive Management - provides general oversight and strategic planning of operations
- Development Team - responsible for delivering a responsive system that fully complies with the functional specification
- System Administrators and IT - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Contact Center - serves customers by providing service that includes resolving product and service issues
- Client Management and Sales - responsible for drafting and executing contracted services for each respective client
- Product Management - responsible for product management, performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts.

Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, Intrusion Detection System ('IDS') alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Output reports are available in electronic portable document format ('PDF'), comma-delimited value file exports, or electronically from the various websites. Reports delivered externally will only be sent using a secure method-encrypted e-mail, secure FTP, or secure websites-to transportation providers, treating facilities, and governments or managed care providers using ACD-developed websites or over connections secured by trusted security certificates. ACD uses Transport Layer Security 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. All teams are expected to adhere to the ACD policies and procedures that define how services should be delivered. These are located on the Company's SharePoint and can be accessed by any ACD team member. All policies are reviewed annually by ACD's Director of IT and IT Supervisor.

Physical Security

The in-scope system and supporting infrastructure is hosted by Flexential. As such, Flexential is responsible for the physical security controls for the in-scope system. Please refer to the Subservice Organizations section below.

Logical Access

ACD uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources.

All assets are inventoried and managed centrally, by ACD's Human Resources ('HR') department. Owners are responsible for approving access to the resource and for performing quarterly reviews of access by role. ACD leverages ADP, the nation's largest payroll processor, and its systems as ACD's primary employee management tool.

Access Review:

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 IT. As part of this process, IT reviews access by privileged roles and requests modifications based on this review.

On an ongoing basis, all access controls are reviewed for each employee and generally for all employees.

As needed, managers review the roles of 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, IT reviews employees with access to privileged roles and requests modifications through Jira.

ACD's new hire process includes the following components:

- Filling out of the new hire provision form by the new manager after formal offer letter sent to new employee
- Background checks, completed W-4, and I-9 reviewed/received before employee start date
- ADP onboarding for employee handbook and policy acknowledgement, as well as payroll processing
- Equipment order and shipment
- First month of training and basecamp new hire checklist, including but not limited to, security training, login/system training, meeting with executive mangers and teammates, etc.

New Hire Provisioning:

ACD requires the completion of the new hire form which denotes which logical access the new hire will need. Form responses are sent directly to the ACD Development Team, creating a ticket in Jira for dev to set-up specific logins and other organizational access.

On an annual basis, access rules for each role are reviewed by a working group composed of IT, Operations ('OPS'), and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Roles are reviewed by the IT Infrastructure Manager and Director of IT, specifically concerning access to data security. 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.

Authentication:

Password authentication and rules are set by requirements related to PCI, SOC2, and HIPAA compliance audits.

All employees access the ACD systems on secure sites through a web browser with specific user credentials. Employee's logins are revoked by a Systems Administration at termination. All access requires two-factor authentication, rigorous password security, as well as additional security tracking utilizing network access control ('NAC') by call registry and constant monitoring. User roles include:

- Executive Management - provides general oversight and strategic planning of operations. Approves user creation and informs System Admins of user roles
- System Administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system. Creates users, grants access. Admins have the highest-level access and must go through multi-factor authentication and additional security protocols
- Contact Center - serves customers by providing service that includes resolving product and service issues. May request user creation through executive management
- Client Management and Sales - responsible for drafting and executing contracted services for each respective client. May request user creation through executive management
- Project Management - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements. May request user creation through executive management

Termination:

At the initiation of an employee's termination of employment, the HR Generalist automatically generates an access deletion record with the IT Infrastructure Manager. This record is routed to the access administrators for deletion.

ACD's Employee Terminations process flow begins with a de-provision notification sent to IT team, specific for disabling access. The employee is then notified of termination and their systems access revocation. The employee ships back any company equipment, final payroll processing takes, and an exit interview is offered and conducted (if employee chooses).

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Sensitive or confidential data (e.g., Cardholder Data: Primary account number ('PAN') and sensitive authentication data) must be protected when stored and when it is in transit over public (or untrusted) networks. Strong industry standard encryption methodologies must be used to protect data stored on hard drives, removable media, backups, etc. ACD follows a strict security policy according to PCI-DSS standards.

Computer Operations - Availability

Incidents or suspected incidents regarding the security of the cardholder data network or cardholder data itself are handled quickly and in a controlled, coordinated, and specific manner, by ACD. An incident response plan is followed in the event of a breach or suspected breach. The following policies specifically address the ACD Incident Response Plan:

- ACD must maintain a documented Incident Response Plan ('IRP') and be prepared to respond immediately to a system breach

- The IRP must clearly define roles and responsibilities for response team members
- The IRP must define communication strategies to be used in the event of a compromise including notification of payment brands
- The IRP must define specific incident response procedures to be followed
- The IRP must document business recovery and continuity procedures
- The IRP must detail all data back-up processes
- The IRP must contain an analysis of all legal requirements for reporting compromises of sensitive data (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise of California resident's data)
- The IRP must address coverage and responses for all critical system components
- The IRP must include or reference the specific incident response procedures from the payment brands
- The IRP must be tested at least annually (maintain evidence that can be validated showing that testing is being performed as per policy)
- ACD must designate specific personnel to be available on a 24/7 basis to respond to alerts. This 24/7 coverage needs to include incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical intrusion detection software ('IDS') alerts, and reports of unauthorized critical system or application file changes
- Require that staff with security breach responsibilities (as defined in the IRP) are trained on their response procedures
- A detailed process and/or procedure for monitoring and responding to alerts from security monitoring systems, including detection of wireless access points, must be defined, and documented in the IRP
- A process must be and is in place for modifying and evolving the IRP according to lessons learned and integrating best practices as the industry develops

ACD uses Flexential monitoring reports and controls to manage data center space, storage, bandwidth, uptime, and overall system efficiency. If the issue is found critical, automation creates a ticket.

Atomic OSSEC reports checked daily, critical issues are brought to immediate attention.

Change Control

ACD 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.

Atlassian's Jira 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. IT Administrators approve changes prior to migration to the production environment and documents those approvals within the ticketing system and Subversion ('SVN').

Beyond Compare is utilized to maintain source code versions and migrate source code through the development process to the production environment. SVN maintains a history of code changes to support rollback capabilities and tracks changes to developers.

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, switches, and servers. If 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. A-LIGN uses an accepted industry standard penetration testing methodology specified by ACD. A-LIGN'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 A-LIGN 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.

Individuals with malicious intent use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities can be fixed by applying vendor-provided security patches. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of sensitive data (cardholder data) by individuals with malicious intent and the use of malicious software.

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

Boundaries of the System

The scope of this report includes the Non-Profit Marketing and Pledge Call Center Services System performed virtually.

This report does not include the data center hosting services provided by Flexential.

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 ACD's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ACD'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 policies communicate the ACD organizational values to personnel. All policies are available on-demand through ACD's company SharePoint and ACD's payroll processor, ADP
- All employees must read and acknowledge the ACD employee handbook, which includes code of conduct, professionalism, and integrity standards

- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

ACD'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

ACD'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 briefed on regulatory and industry changes affecting the services provided at least on an annual basis
- 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

ACD'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.

ACD'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 will be 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

HR Policies and Practices

ACD'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. ACD's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

ACD's employee management components include (but are not limited to): annual performance review through ADP, annual (if not more frequent) security trainings, annual equipment inventories, annual (if not more frequent) security scans, annual benefit enrollment and review, monthly webinars and all-hands meetings, and quarterly performance check-ins (if needed).

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

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- All employees go through annual trainings, including security
- All employee systems go through security scans at least annually
- 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

ACD's risk assessment process identifies and manages risks that could potentially affect ACD's ability to provide reliable contact center services to non-profit organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ACD identifies the underlying sources of risk, measures the impact to 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 ACD, 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 non-profit industry
- Compliance - legal and regulatory (PCI / SOC2) changes

ACD has established a lawyer on retainer and a compliance point person 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 non-profit marketplace. ACD does actively identify and mitigate significant risks through the implementation of various security initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ACD's Non-Profit Marketing and Pledge Call Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. ACD addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ACD's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of ACD'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 ACD, 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, company-wide meetings are held monthly through Microsoft Teams to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the company-wide 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 ACD personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. ACD'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 is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

ACD's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon 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 ACD'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 ACD's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going 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.

Risk Assessments

ACD has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by ACD to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the Director of IT and IT Infrastructure Manager at least on an annual basis:

- Risk Assessment: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines, and quality
- Health Information Security Risks: Health information security risks are assessed by Director of IT. Risk factors associated with the organization are evaluated considering compliance obligations, laws, and regulations, policies, and procedures, contracts, and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the Director of IT and IT Supervisor of the organization

Significant 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.

Significant 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 criterion was applicable to the Non-Profit Marketing and Pledge Call Center Services System.

Subservice Organizations

This report does not include the data center hosting services provided by Flexential.

Subservice Description of Services

Flexential provides data center hosting services for ACD. Flexential provided added security such as physical data center security, formal access procedures, as well as equipment delivery and storage.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Flexential to provide additional assurance that the trust services criteria requirements described within this report are met:

Subservice Organization - Flexential		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: • Access card and PIN at building entrances • Access card and biometric scan at data center entrance
		Visitors are required to wear a visitor badge while visiting the data centers.
		Data center visitors are required to be accompanied and supervised by an authorized Flexential employee or client escort.
		Visitors are required to sign-in with onsite security personnel prior to entering the data centers.
		Client equipment is maintained in lockable cages or racks within the data centers.
		Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.
		The Director of Compliance, at Flexential, reviews user account access of terminated employees.
		A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.
		Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following: • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging
		The data centers are equipped with fueled electric power generators to provide backup power in the event of a power outage.
		The data centers are connected to multiple redundant uninterruptible power supply ('UPS') systems configured to provide temporary electricity in the event of a power outage.

ACD 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, ACD 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 by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to ACD.
2. User entities are responsible for notifying ACD of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management, and control of the use of ACD services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ACD services.
5. User entities are responsible for providing ACD with a list of approvers for security and system configuration changes for data transmission.
6. User entities are responsible for immediately notifying ACD of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security 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 removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Activities Specified by the Service Organization

The applicable trust 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 criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of ACD's description of the system. Any applicable trust services criteria that are not addressed by control activities at ACD are described within Section 4.

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

SECTION 4

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

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

A-LIGN ASSURANCE's examination of the controls of ACD was limited to the Trust Services Criteria, related criteria and control activities specified by the management of ACD and did not encompass all aspects of ACD'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 SharePoint 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 acknowledgement tracking spreadsheet 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.
		Prior to employment, personnel are required to complete a background check.	Inspected the background check policies and procedures and the completed background check 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.

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**
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook acknowledgement tracking spreadsheet 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 policies to determine that sanction policies, which include 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 employee handbook and reporting tool to determine that employees were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed on an annual basis.	Inspected the executive management job descriptions including revision dates to determine that executive management roles and responsibilities were documented and 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**
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the performance evaluation tracking spreadsheet for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		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 compliance summary 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.

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 evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the evaluation tracking spreadsheet for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	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 within the environment.	No exceptions noted.
			Inspected the compliance summary meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		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 report 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.

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**
CC1.3	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 SharePoint site.	Inspected a sample of job descriptions and the entity's SharePoint to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history for a sample of job descriptions 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 and code of conduct.	Inspected the signed employee handbook acknowledgement tracking spreadsheet 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.

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 has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, internal controls matrix, and a sample of job descriptions to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected a sample of job descriptions to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures to determine that a vendor risk assessment was required on an annual basis.	No exceptions noted.
			Inspected the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Executive management considers the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions.	Inspected the organizational chart and a sample of job descriptions to determine that executive management considered the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance 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.
		The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	Inspected the resumes 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 a sample of job descriptions and the resumes 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the entities recruiting forms to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training outline to determine that executive management created a training program for its employees.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it relates to their job role and responsibilities.	No exceptions noted.
		Prior to employment, personnel are required to complete a background check.	Inspected the background check policies and procedures and the completed background check 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.

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**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected a sample of job descriptions and the entity's SharePoint to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook acknowledgement tracking spreadsheet 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 acknowledgement tracking spreadsheet 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.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance 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.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the revision history for a sample of job descriptions to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.
		Sanction policies which include probation, suspension and termination are in place for employee misconduct.	Inspected the sanction policies 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 SharePoint site.	Inspected the entity's SharePoint and internal resource page 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 SharePoint site.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected an example edit check configuration to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	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 the entity's network flow diagram 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 file integrity monitoring ('FIM') configurations, IDS 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.

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**
		Data is only retained for as long as required to perform the required system functionality, service, or use.	Inspected the data retention policies and procedures to determine that data was retained for only as long as required to perform the required system functionality, service, or use.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected a sample of job descriptions and the entity's SharePoint to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's ADP portal and SharePoint site.	Inspected the entity's SharePoint and internal resource page to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the entity's ADP portal and SharePoint site.	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 manual handbook, security training report, and performance review report 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.

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**
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook acknowledgement tracking spreadsheet 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 and code of conduct.	Inspected the signed employee handbook acknowledgement tracking spreadsheet 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.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the entity's strategy map and plan to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report issues and concerns.	Inspected the employee handbook and reporting tool to determine that employees, third-parties and customers were directed on how to issues report and concerns.	No exceptions noted.
		Changes to job roles and responsibilities are communicated to personnel through updated job descriptions.	Inspected the company newsletters sent via e-mail to determine that changes to job roles and responsibilities were communicated to personnel through updated job descriptions.	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 SharePoint site.	Inspected the incident response policy on the company's SharePoint 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 SharePoint site.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's e-mail.	Inspected the company newsletters sent via e-mail to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's e-mail.	No exceptions noted.
		Employees are required to attend security awareness training annually.	Inspected the IT security training report 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 IT security training report to determine that management tracked and monitored compliance with information security and awareness training requirements.	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**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the entity's SharePoint and internal resource page to determine that the information security policies and procedures that communicate the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties.	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement 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 agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via mass e-mail notifications.	Inspected the company newsletters sent via e-mail to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users, and customers via mass e-mail notifications.	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**
		Executive management meets annually with operational management to discuss the results of assessments performed by third-parties.	Inspected the compliance summary 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, third-parties, and customers are directed on how to report issues and concerns.	Inspected the employee handbook and reporting tool to determine that employees, third-parties and customers were directed on how to issues report and concerns.	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, employee performance policies and procedures 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 assessment and management policies and procedures 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 reviews policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the entity’s objectives and control documentation to determine that executive management reviewed policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	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**
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the strategic plan balanced scorecard 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.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and a sample of job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the entity's KPI's to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness 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.

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**
		Executive management reviews operational and resourcing reports to evaluate performance and resourcing at least annually.	Inspected the strategic plan balanced scorecard to determine that executive management reviewed operational and resourcing reports to evaluate performance and resourcing at least annually.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the strategic objectives and budgets 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 strategic objectives and budgets to determine that entity strategies, objectives and budgets were assessed on an annual basis.	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.
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 assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a 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**
		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 assessment and management policies and procedures 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 assessment and management policies and procedures 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 Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures 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.
		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 assessment and management policies and procedures 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.

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 annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policies and procedures 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.
		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 assessment and management policies and procedures 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.

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 incentives, pressures, 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 incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	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 assessment and management policies and procedures 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.

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 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 assessment and management policies and procedures 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.
		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 assessment and management policies and procedures 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				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes in vendor and third-party relationships 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 vendor and third-party relationships 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 system configurations, the antivirus schedule configurations, the FIM configurations, the IDS log, and the 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.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the information security policy and the incident response policy to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
			Inspected the compliance summary meeting minutes to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	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 the compliance summary 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.

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**
		Logical access reviews and backup restoration tests are performed on a quarterly basis and at least annually, respectively.	Inspected the user access review for a sample of quarters to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	No exceptions noted.
			Inspected the backup restoration test to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	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.
		Evaluations of policies, controls, systems, tools, applications, and third-parties for effectiveness and compliance is required at least annually.	Inspected the revision history of entity policies and procedures to determine evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
			Inspected the compliance summary meeting minutes to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's completed attestation reports to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
			Inspected the completed risk assessment to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
		Management reviews the frequency of compliance evaluations annually and adjusts it based on changes to the environment and operational performance.	Inspected the compliance summary meeting minutes to determine that management reviewed the frequency of compliance evaluations annually and adjusted it based on changes to the environment and operational performance.	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.
		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.

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**
		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 vendor management policy and completed attestation report for a sample of vendors with an attestation report 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.
		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.
		Evaluations are performed by individuals with sufficient knowledge of what is being evaluated.	Inspected the internal control matrix to determine that evaluations were performed by individuals with sufficient knowledge of what was being evaluated.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the compliance summary meeting minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	Inspected the compliance summary meeting minutes to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk and attestation assessments to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting resolution documentation for vulnerabilities identified from a sample of vulnerability scans to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.	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**
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.	Inspected the completed risk and attestation assessments to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were documented, investigated, and addressed.	No exceptions noted.
			Inspected the supporting resolution documentation for vulnerabilities identified from a sample of vulnerability scans to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were documented, investigated, and addressed.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.	Inspected the completed risk and attestation assessments to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were addressed by those parties responsible for taking corrective actions.	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 supporting resolution documentation for vulnerabilities identified from a sample of vulnerability scans to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk 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 compliance summary meeting minutes and the PCI executive reports 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 attestation 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 supporting resolution documentation for vulnerabilities identified from a sample of vulnerability scans 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.

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**
		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.
		Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations.	Inspected the internal controls matrix to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature, and scope of its operations.	No exceptions noted.
			Inspected the compliance summary meeting minutes to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature, and scope of its operations.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine management documented the relevant controls in place for each key business or operational process.	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 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 include 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 assessment and management policies and procedures 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 plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested 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**
		As part of the business continuity process, IT review checklists are performed on a quarterly basis.	Inspected the IT review checklist for a sample of quarters to determine that as part of the business continuity process, IT review checklists were performed on a quarterly basis.	No exceptions noted.
		As part of the business continuity process, backups are restored to production on a weekly basis.	Inspected the backup restoration configurations to determine that as part of the business continuity process, backups were restored to production on a weekly basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and internal controls matrix to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	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.

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**
		Organizational and information security policies and procedures are documented and made available to employees through the entity's SharePoint site.	Inspected the information security policy and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	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 incomplete, inaccurate, and 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 incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	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 employees through the entity's SharePoint site.	Inspected the information security policy and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	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 information security policies, incident response policies 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.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected a sample of job descriptions and the entity's SharePoint to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	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**
		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 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.
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected the compliance summary meeting minutes to determine that effectiveness of the internal controls implemented within the environment were evaluated annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the IT Infrastructure Manager regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the networks, database, applications, and VPN to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine 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.

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 administrative access is restricted.	Inquired of the IT Infrastructure Manager regarding privileged access the network to determine that network administrative access was restricted.	No exceptions noted.
			Inspected the network administrator listing to determine that network administrative access was restricted.	No exceptions noted.
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity	No exceptions noted.
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Reset counter	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Reset counter	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 • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events	Inspected the network audit logging settings and an example network log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account Management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed if-needed.	Inquired of the IT Infrastructure Manager regarding the network audit logging process to determine that network audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected the network audit logging settings and an example network log extract to determine that network audit logs were maintained and reviewed if-needed.	No exceptions noted.
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing to determine that database 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 administrative access is restricted.	Inquired of the IT Infrastructure Manager regarding the database administrators to determine that database administrative access was restricted.	No exceptions noted.
			Inspected the database administrator listing to determine that database administrative access was restricted.	No exceptions noted.
		Databases are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity	Inspected the database password settings to determine that database was configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity	No exceptions noted.
		Database users are authenticated via individually-assigned user accounts and passwords.	Observed the IT Infrastructure Manager 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 duration • Account lockout threshold • Reset counter	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Reset counter	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 audit logging settings are in place that include: • Account logon events • Account logoff events • Failed authentications • Invalid User Attempts	Inspected the database audit logging settings and an example database log extract to determine that database audit logging configurations were in place that included: • Account logon events • Account logoff events • Failed authentications • Invalid User Attempts	No exceptions noted.
		Database audit logs are maintained and reviewed if-needed.	Inquired of the IT Infrastructure Manager regarding the database audit logging process to determine the database audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected the database audit logging settings and an example database log extract to determine that database audit logs were maintained and reviewed if-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.	Inquired of the IT Infrastructure Manager regarding the application administrators to determine that application administrative access was restricted.	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 application administrator listing to determine that application administrative access was restricted.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password length • Complexity	No exceptions noted.
		Application users are authenticated via individually-assigned user accounts and passwords.	Observed the IT Infrastructure Manager 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 duration • Account lockout threshold	Inspected the application account lockout settings to determine that application account lockout settings were in place that include: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Application audit policy settings are in place that include: • Account management • Error Logs	Inspected the application audit logging settings and an example application log extract to determine that application audit logging configurations were in place that included: • Account management • Error Logs	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 if-needed.	Inquired of the IT Infrastructure Manager regarding application logging to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected the application audit logging settings and an example application log extract to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
	Remote Access			
		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.	Inquired of the IT Infrastructure Manager regarding VPN administrative access to determine that the ability to administer VPN access was restricted.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Observed the IT Infrastructure Manager authenticate through the VPN to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the 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**
			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.
		VPN account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Reset Counter	Inspected the VPN account lockout settings to determine that application account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Reset Counter	No exceptions noted.
		VPN logging settings are in place, covering, that include: • Successful Login events • Failed Login events	Inspected the VPN logging configurations and a VPN log extract to determine that VPN logging settings were in place, that include: • Successful Login events • Failed Login events	No exceptions noted.
		VPN audit logs are maintained and available for review if needed.	Inquired of the IT Infrastructure Manager regarding reviewing VPN logs to determine that VPN audit logs were maintained and available for review if needed.	No exceptions noted.
			Inspected the VPN logging configurations and a VPN log extract to determine that VPN audit logs were maintained and available for review if 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**
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the network diagram, the firewall rulesets, and the DMZ settings to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IDS.	Inspected IDS 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 IDS.	No exceptions noted.
		Server certificate-based authentication is used as part of the Secure Socket Layer/ Transport Layer Security ('SSL/TLS') encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inspected the encryption policy to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews and backup restoration tests are performed on a quarterly basis and at least annually, respectively.	Inspected the user access review for a sample of quarters to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	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 backup restoration test to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	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 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 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.

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**
CC6.2	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 policy to determine 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 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 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 and backup restoration tests are performed on a quarterly basis and at least annually, respectively.	Inspected the user access review for a sample of quarters to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	No exceptions noted.
			Inspected the backup restoration test to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	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**
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the IT Infrastructure Manager regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the networks, database, applications, and VPN to determine that privileged access to sensitive resources was restricted to authorized personnel.	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 policy to determine 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 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 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.

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**
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the IT Infrastructure Manager regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the networks, database, applications, and VPN to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews and backup restoration tests are performed on a quarterly basis and at least annually, respectively.	Inspected the user access review for a sample of quarters to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	No exceptions noted.
			Inspected the backup restoration test to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	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.

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 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 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 customer credit card information disposal.	Inspected the information security policy and the data retention storage procedures to determine policies and procedures were in place to guide personnel in customer credit card information disposal.	No exceptions noted.
		Data that is no longer required for business purposes is removed from storage locations.	Inquired of the IT Infrastructure Manager regarding the data disposal process to determine data that was no longer required for business purposes was removed from storage locations.	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 data retention storage procedures and procedures to determine data that was no longer required for business purposes was removed from storage locations.	No exceptions noted.
			Inspected the service ticket for a sample of requests to dispose of data to determine that data that was no longer required for business purposes was removed from storage locations.	Testing of the control activity disclosed that there were no requests for data disposal that occurred during the review period.
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, SSL, and other encryption technologies are used for defined points of connectivity.	Inspected encryption configurations, VPN authentication configurations and digital certificates to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Observed the IT Infrastructure Manager authenticate through the VPN to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the 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**
			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 SSL/TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	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, password, and multi-factor authentication before establishing a VPN session.	Observed the IT Infrastructure Manager authenticate through the VPN to determine that remote connectivity users were authenticated via an authorized user account, password, and multi-factor authentication before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account, password, and multi-factor authentication 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**
		Logical access to stored data is restricted to authorized personnel.	Inquired of the IT Infrastructure Manager regarding database administrative access 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 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 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 firewall rule sets for the production servers to determine 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**
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example alert e-mail to determine that the IDS was configured to notify personnel upon intrusion detection.	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 is configured to automatically push updates to the installed antivirus software daily.	Inspected the antivirus settings to determine that the antivirus software provider was configured to automatically push updates to the installed antivirus software daily.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	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 IT Infrastructure Manager regarding database administrative access 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.
		The ability to access the datacenter and recall backed up data is restricted to authorized personnel.	Inquired of the IT Infrastructure Manager regarding recalling backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the list of users with the ability to recall backup media from the third-party storage facility to determine that the ability to access the datacenter and recall 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 IDS, antivirus software and a DMZ.	Inspected the network diagram, IDS 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 IDS, antivirus software and a DMZ.	No exceptions noted.
		VPN, SSL, and other encryption technologies are used for defined points of connectivity.	Inspected encryption configurations, VPN authentication configurations and digital certificates to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account, password, and multi-factor authentication before establishing a VPN session.	Observed the IT Infrastructure Manager authenticate through the VPN to determine that remote connectivity users were authenticated via an authorized user account, password, and multi-factor authentication 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, password, and multi-factor authentication 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 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 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 firewall rule sets for the production servers to determine 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 IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example alert e-mail to determine that the IDS was configured to notify personnel upon intrusion detection.	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.	Inquired of the IT Infrastructure Manager regarding the ability to push changes into the production environment to determine that the ability to migrate changes into the production environment was restricted.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine FIM software was in place to ensure only authorized changes were deployed into the production environment.	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 FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change control procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Documented vulnerability policies and procedures are in place to guide personnel in the vulnerability discovery process.	Inspected the vulnerability discovery and risk ranking policy to determine that documented vulnerability policies and procedures were in place to guide personnel in the vulnerability discovery process.	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 is configured to automatically push updates to the installed antivirus software daily.	Inspected the antivirus settings to determine that the antivirus software provider was configured to automatically push updates to the installed antivirus software daily.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a daily 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**
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.	Management has defined configuration standards in the information security policies and procedures.	Inspected the information security policy to determine that management had defined configuration standards in the information security policies and procedures.	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 system configurations, the antivirus schedule configurations, the FIM configurations, the IDS log, and the 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, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS 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 IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example alert e-mail to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine FIM software was in place to ensure only authorized changes were deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the information security policy 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 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 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 firewall rule sets for the production servers to determine 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 the information security and incident response procedures to determine policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.	Inspected the vulnerability scan results for a sample of months and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on at least an annual basis and remedial actions were taken where necessary.	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 response procedures to determine documented 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 the information security and incident response procedures to determine 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, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring system configurations, the antivirus schedule configurations, the FIM configurations, the IDS log, and the 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.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example alert e-mail to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine FIM software was in place to ensure only authorized changes were deployed into the production 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**
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		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 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 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 firewall rule sets for the production servers to determine 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**
		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 is configured to automatically push updates to the installed antivirus software daily.	Inspected the antivirus settings to determine that the antivirus software provider was configured to automatically push updates to the installed antivirus software daily.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.
	Network			
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Reset counter	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Reset counter	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 • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events	Inspected the network audit logging settings and an example network log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account Management • Directory service access • Logon events • Object access • Policy change • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as-needed.	Inquired of the IT Infrastructure Manager regarding the network audit logging process to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected the network audit logging settings and an example network log extract to determine that network audit logs were maintained and reviewed as-needed.	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			
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Reset counter	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Reset counter	No exceptions noted.
		Database audit logging settings are in place that include: • Account logon events • Account logoff events • Failed authentications • Invalid User Attempts	Inspected the database audit logging settings and an example database log extract to determine that database audit logging configurations were in place that included: • Account logon events • Account logoff events • Failed authentications • Invalid User Attempts	No exceptions noted.
		Database audit logs are maintained and reviewed if-needed.	Inquired of the IT Infrastructure Manager regarding the database audit logging process to determine the database audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected the database audit logging settings and an example database log extract to determine that database audit logs were maintained and reviewed if-needed.	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			
		Application audit policy settings are in place that include: • Account management • Error Logs	Inspected the application audit logging settings and an example application log extract to determine that application audit logging configurations were in place that included: • Account management • Error Logs	No exceptions noted.
		Application audit logs are maintained and reviewed if-needed.	Inquired of the IT Infrastructure Manager regarding application logging to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected the application audit logging settings and an example application log extract to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
		Management monitors the effectiveness of detection tools and controls implemented within the environment.	Inspected the compliance summary meeting minutes to determine that management monitored the effectiveness of detection tools and controls implemented within the environment.	No exceptions noted.
		Part of this criterion is responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 response procedures to determine documented 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 response procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response procedures to determine that the incident response policies and procedures 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.	Inspected the incident response procedures to determine resolution of incidents were required to be documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine resolution of incidents were 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**
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Identified incidents are reviewed, monitored, and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of incidents to determine identified incidents were reviewed, monitored, and investigated by an incident response team.	No exceptions noted.
		Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including the determination and execution of the containment approach.	Inspected the incident response procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including 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 the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		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 response procedures to determine documented 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.	Inspected the supporting incident ticket for a sample of incidents to determine incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inspected the supporting incident ticket for a sample of incidents to determine the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response procedures 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.

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**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including the determination and execution of the containment approach.	Inspected the incident response procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including 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 the determination and execution of the containment approach.	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 risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting resolution documentation for vulnerabilities identified from a sample of vulnerability scans to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policy to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the change control procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	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 entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change control procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies to determine that data backup procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups are performed on a weekly basis and differential backups are performed daily.	Inspected the backup schedule configurations and an example backup log to determine that full backups were performed on a weekly basis and differential backups were performed daily.	No exceptions noted.
		Logical access reviews and backup restoration tests are performed on a quarterly basis and at least annually, respectively.	Inspected the user access review for a sample of quarters to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	No exceptions noted.
			Inspected the backup restoration test to determine that logical access reviews and backup restoration tests were performed on a quarterly basis and at least annually, respectively.	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**
		On an annual basis, preventative and detective controls are evaluated and changed as necessary.	Inspected the compliance summary meeting minutes to determine that on an annual basis, preventative and detective controls were evaluated and changed as necessary.	No exceptions noted.
			Inspected the entity's completed attestation reports to determine that on an annual basis, preventative and detective controls were evaluated and changed as necessary.	No exceptions noted.
		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 plans 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 an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		As part of the business continuity process, IT review checklists are performed on a quarterly basis.	Inspected the IT review checklist for a sample of quarters to determine that as part of the business continuity process, IT review checklists were performed on a quarterly 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**
		As part of the business continuity process, backups are restored to production on a weekly basis.	Inspected the backup restoration configurations to determine that as part of the business continuity process, backups were restored to production on a weekly basis.	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 control policies and procedures 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- executive ACD personnel • Development - development team • Testing-quality assurance department • Implementation - software change management group	Inspected the change control policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests- executive ACD personnel • Development-development team • Testing-quality assurance department • Implementation - software change management group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the systems enhancement alert e-mails 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.	Inquired of the IT Infrastructure Manager regarding access to implement changes to determine that access to implement changes in the production environment was restricted.	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 list of users with access to deploy changes into the production environment and user review for domain administrators to determine that access to implement changes in the production environment was restricted.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change tickets for a sample of system 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 SVN log 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.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development 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 change tickets for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.	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**
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes were deployed into the production environment.	No exceptions noted.
		Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation.	Inspected the supporting change tickets for a sample of system changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	No exceptions noted.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change tickets for a sample of system 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.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change control policies and procedures 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 assessment and management policies and procedures 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 assessment and management policies and procedures 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 assessment and management policies and procedures 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**
			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.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures 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.
		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 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 risk assessment policies and procedures 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.

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**
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor risk assessment policies and procedures to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
			Inspected the completed vendor risk assessment 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 risk assessment policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the completed vendor risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party 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**
		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 vendor management policy and completed attestation report for a sample of critical vendors with an attestation report 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.
		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 risk assessment policies and procedures 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.
		Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	Inspected the organizational chart and a sample of job descriptions to determine that management assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	No exceptions noted.