A-LIGN

A-LIGN.com

Type 2 SOC 2

Prepared for:
Prog Leasing, LLC

Year:
2025

Progressive Leasing®

REPORT ON PROG LEASING, LLC'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY

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, 2024 to June 30, 2025

Table of Contents

SECTION 1

ASSERTION OF PROG LEASING, LLC MANAGEMENT

ASSERTION OF PROG LEASING, LLC MANAGEMENT

July 23, 2025

We have prepared the accompanying description of Prog Leasing, LLC's ('Prog Leasing' or 'the Company') Lease to Own Services System titled "Prog Leasing, LLC's Description of Its Lease to Own Services System throughout the period July 1, 2024 to June 30, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria)*.* The description is intended to provide report users with information about the Lease to Own Services System that may be useful when assessing the risks arising from interactions with Prog Leasing's system, particularly information about system controls that Prog Leasing has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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)* and Prog Leasing's compliance with the commitments in its Privacy Notice throughout the period July 1, 2024 to June 30, 2025.

Prog Leasing uses Amazon Web Services ('AWS') to provide cloud hosting services and Flexential to provide data center and cloud operations services (collectively, 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Prog Leasing, to achieve Prog Leasing's service commitments and system requirements based on the applicable trust services criteria and Prog Leasing's compliance with the commitments in its Privacy Notice. The description presents Prog Leasing's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Prog Leasing's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents Prog Leasing's Lease to Own Services System that was designed and implemented throughout the period July 1, 2024 to June 30, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Prog Leasing'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 Prog Leasing's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Prog Leasing'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 Prog Leasing's controls operated effectively throughout that period.

d. we complied with the commitments within the Privacy Notice, in all material respects, throughout the period July 1, 2024 to June 30, 2025.

Diego Souza
Chief Information Security Officer
Prog Leasing, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Prog Leasing, LLC

Scope

We have examined Prog Leasing's accompanying description of its Lease to Own Services System titled "Prog Leasing, LLC's Description of Its Lease to Own Services System throughout the period July 1, 2024 to June 30, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Prog Leasing's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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*) and Prog Leasing's compliance with the commitments in its Privacy Notice throughout the period July 1, 2024 to June 30, 2025.

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

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

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

Service Organization’s Responsibilities

Prog Leasing 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 Prog Leasing’s service commitments and system requirements were achieved. Prog Leasing has provided the accompanying assertion titled "Assertion of Prog Leasing, LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Prog Leasing 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 and complying with the commitments in its Privacy Notice that is included in the description.

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 and its compliance with the commitments in its Privacy Notice. 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 and its compliance with the commitments in its Privacy Notice
- 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 and its compliance with the commitments in its Privacy Notice
- Evaluating the overall presentation of the description

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects,

a. the description presents Prog Leasing's Lease to Own Services System that was designed and implemented throughout the period July 1, 2024 to June 30, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Prog Leasing'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 Prog Leasing's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Prog Leasing'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 Prog Leasing's controls operated effectively throughout that period.
d. Prog Leasing's compliance with the commitments in its Privacy Notice throughout the period July 1, 2024 to June 30, 2025.

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 Prog Leasing, user entities of Prog Leasing's Lease to Own Services System during some or all of the period July 1, 2024 to June 30, 2025, business partners of Prog Leasing subject to risks arising from interactions with the Lease to Own 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 and its commitments in its Privacy Notice
- The applicable trust services criteria and its commitments in its Privacy Notice
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and its commitments in its Privacy Notice 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
July 23, 2025

SECTION 3

PROG LEASING, LLC'S DESCRIPTION OF ITS LEASE TO OWN SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2024 TO JUNE 30, 2025

OVERVIEW OF OPERATIONS

Company Background

In 1999, Progressive Leasing introduced the world to virtual lease-to-own purchase options. This easily integrated service enabled retailers to provide alternative lease-purchase options to consumers with less than perfect credit. Working with some of the largest retailers in the USA, Progressive Leasing has helped millions of people get the things they need with ease.

Description of Services Provided

The Progressive Leasing software as a service (SaaS) platform allows retailers to offer shoppers a lease-to-own purchase option both in store and online.

The retailer platform is comprised of three primary components: Apply, Lease, and Checkout:

- Apply: Allows a shopper to enter their information and submit an application for a lease.
- Lease: A unique lease is created for every retail purchase. The lease technology allows a customer and/or retailer to create a lease with specific items. Each lease includes terms that conform to the state laws where the lease is being completed. A digital lease document is generated instantly for a customer to sign and submit to Progressive Leasing online. An online initial payment service is also part of the lease signing session.
- Checkout: Once a lease is signed, Progressive Leasing has a variety of mechanisms by which to fund a retailer for the purchase of the item or allow the retailer to tender a transaction and submit invoice to Progressive Leasing. In addition, there are numerous returns and exchange technologies that are accessed by retailers to facilitate such transactions.

Shoppers can also apply for a lease online through either a downloadable mobile application or the Progressive Leasing website.

Customers can also manage their lease account and payments online via the MyAccount website.

Principal Service Commitments and System Requirements

Progressive Leasing serves two main stakeholders: (1) merchants in various consumer goods verticals such as furniture, mattress, jewelry, tires and wheels, mobile devices, and appliance; and (2) consumers that apply for and lease the goods that Progressive Leasing buys from merchants to make available under lease-to-own agreements governed by state laws.

Progressive Leasing has partnered with merchants throughout the United States. These partnerships require merchants to comply with guidelines, referred to as “Retailer Procedures,” which Progressive Leasing makes available online and through specific training that is provided when necessary. The Retailer Procedures require compliance with minimum requirements for confidentiality, privacy, tax matters, and other legal issues applicable to this industry. Progressive Leasing monitors and follows-up with any instances of non-compliance by retailers.

In addition, Progressive Leasing has invested in an industry-leading platform to meet sales, use, and property tax requirements and to make sure the agreements and interactions with the consumers meet any requirements which may apply.

Approve.Me is an application platform affiliated with Progressive Leasing that some consumers use as part of the application process. Under certain retail partnerships, a consumer may consent to have their application information sent from Approve.Me to lenders as part of a decisioning “waterfall,” which allows a consumer to be considered for financing through such lenders, in addition to being considered for a lease agreement with Progressive Leasing. A merchant may tailor the flow of the waterfall based on their preference and in compliance with Retailer Procedures. Under other retail partnerships, Approve.Me facilitates sending the application directly to Progressive Leasing to be considered for a lease agreement.

Components of the System

Infrastructure

Primary infrastructure used to provide Prog Leasing's Lease to Own Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Blade Servers	HPE ProLiant Blades	Host VMs (Virtual Machine) running production applications and databases
Storage Arrays	Pure, NetApp Nimble	Provides storage for VMs and applications
Backup Appliance	Exagrid, NetApp	Backup target for VMs and data backups
Switches	Cisco Nexus and Catalyst switches	Provides networking for corporate and production networks
Firewalls	Palo Alto	Filters traffic into and out of the corporate and production networks according to specified policies
Load Balancers	F5 BIG-IP 4000	Acts as a reverse proxy and distributes application traffic across redundant servers for high availability

Software

Primary software used to provide Prog Leasing's Lease to Own Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
VMWare vCenter, vSphere	ESXi 6.7	Software to run and manage virtual machines
Microsoft Office 365	Azure Cloud	E-mail and office productivity applications
Veeam Backup and Recovery	Windows Server 2012 R2 / 2016	Manages backups of VMs
CyberArk	Hosted	Password Management
Microsoft SQL Server	Windows Server 2012 R2/2016	Production databases
ConnectWise	Windows Server 2012 R2 / 2016	Remote administration and Patch management
Microsoft Active Directory (AD)	Windows Server 2012 R2 / 2016	Identity Access Management
AD Audit	Windows Server 2012 R2 / 2016	Audit changes to AD and server environment
Splunk, Dynatrace	CentOS 7	Server and application logging
Zerto	ESXi 6.7	Disaster recovery

Primary Software		
Software	**Operating System**	**Purpose**
Zabbix	CentOS 7	Network Monitoring System
Enterprise Supporting Services	Windows Server 2012 R2	Domain controller / Domain services

People

Progressive Leasing has 1,600 employees who work for the following departments: Operations, Sales, Marketing, Technology, Finance, Legal, Human Resources, and Compliance:

- Human Resources: This team is known as the People team and has oversight for strategic planning, development, implementation, administration and management of the company's talent and culture strategies and programs, including recruitment, talent management, diversity initiatives, performance management, employee relations, compensation and benefits, training, leadership development, internal communications, philanthropic/community activities, employee events and employee engagement. The team is responsible for establishing long-range human resource strategies and practices, ensuring business processes comply with regulatory and legal requirements, minimizing risk to the organization.
- Operations: Staff that is responsible for handling front-line communications with Progressive Leasing customers and retail partners through various departments (i.e. Customer Support, Merchant Support, Customer Payment Specialist). They provide support on the services, quality assurance, and reliable service levels through monitoring and reporting.
- Sales and Marketing: The Sales department is a direct link to Progressive Leasing retail partners who promote the services to new and existing retailers. The staff are trained well to assist Prog Leasing retail partners with exceptional service throughout the entire relationship. The Marketing department assists the Sales team by providing up-to-date and attractive materials and advertising.
- Technology: Teams involved in the hardware, software, architecture, security, and networking in the organization (i.e. Service Desk, Software Engineering, Infrastructure, information Security, Database Engineering). These teams are responsible for the creation and maintenance of the applications and systems used by Progressive Leasing, customers, retailer partners, and vendors.
- Compliance and Legal: These teams are responsible for the policies and procedures based on applicable law and industry best practices.

Data

Progressive Leasing systems utilize Microsoft SQL Server as the primary engine for the management of databases. Microsoft SQL Server is Progressive Leasing's core service for storing, processing, and securing data. Data is stored in relational models over numerous database structures and files. Software systems accessing the database use SQL Server Native Client .NET or OLE DB client driver implementations. Progressive Leasing utilizes Transport Layer Security (TLS) for internal database network connections. Database actions utilize stored procedures to access any data within, to ensure parameterized execution. Data access is isolated and granted on a justified business need basis. Error logs are extracted to Progressive Leasing's centralized logging platform.

Databases have a set regular schedule for backup recovery and utilize a highly available clustering solution to prevent data loss. Database components are monitored and audited for changes to structure definition. Key data components are monitored and audited for modifications to data content.

Large data extract, transform, and load (ETL) solutions are handled by SQL Server Integration Services (SSIS) through secure connections. Any files with external consumption to or from external origin are encrypted using Pretty Good Privacy encryption algorithms with key pairs isolated by process.

Privacy Commitments

The following table describes the information collected by Progressive Leasing's application platforms:

Client Data
• Name • Address • Telephone number • E-mail address • Date of birth • Social security number • Driver's license or other personal identification numbers • Bank account and other financial institution account numbers • Vehicle information • Occupation and employment information • Source of income • Personal references • Residence

The online privacy policy ("Privacy Policy") describes how Progressive Finance Holdings, LLC, Prog Leasing, LLC, AM2 Enterprises, LLC, and each of their affiliates, subsidiaries, and divisions collect, use and disclose user information. Customers read and consent to the Privacy Policy as part of their application process. See Progressive Leasing's Privacy Policy at https://progleasing.com/privacy.

The Privacy Policy applies to Progressive Leasing's websites, kiosks, applications, and other online services that post or include a link to this Privacy Policy (collectively, the "Progressive Platforms"). In addition to this Privacy Policy, customers review and consent to the Terms of Use, which governs the customers use of the Progressive Platforms, and the Application Disclosure, which governs the customers submission of a lease-to-own application submitted to Progressive Leasing, and the Arbitration Provision, which includes the customer agreement to arbitrate any disputes with Progressive, customer waiver to bring class action suits, and other important information.

<u>Definitions - Information Collected</u>

As stated in the Privacy Policy, Progressive Leasing collects from customers certain information, including "Personal Information" from customers, such as name, address, telephone number, e-mail address, social security number, and bank account or other financial institution account numbers. Progressive Leasing also collects "Non-Personal- Information" such as vehicle information, occupation and other employment information, source of income, personal references, residence related- information such as lease and ownership information, and "Usage Information." Usage Information may include the URL or advertisement that referred customers to the Progressive Platforms, the areas within the Progressive Platforms that customers visit, location information, and mobile network (if applicable), among other similar information. In addition, Progressive Leasing may collect the hardware model, browser, and operating system that customers are using and IP addresses or other unique device identifiers ("Device Information") for any computer, mobile phone or other device that is used to access the Progressive Platforms. In some cases, Progressive Leasing may directly collect location information through personal devices. Customers may be able to turn off the collection of location information through the settings on their personal device. Usage information is generally nonidentifying-, but if Progressive Leasing associates use it with a specific and indefinable user, Progressive Leasing treats it as personal information. Personal Information, Non-Personal- Information, Usage Information, and Device Information are included in the definition of the term "information" when it is used in the Privacy Policy.

Choice-Customer Options Concerning Their Information

The Privacy Policy affords customers certain options concerning their information. The Privacy Policy states:

a. Accessing and Correcting Personal Information. You may request access or update the Personal Information that we hold about you. You can access or update your Personal Information in the following ways:
    i. If you have created an account on the Progressive Platforms, you will be able to update your own contact and payment information, subject to certain limitations.
    ii. Contact us through one of the methods listed in the “How Can You Contact Us?” section within this Privacy Policy. Please include your current contact information, the information that you are interested in accessing, and your requested changes. After authenticating your request, we will provide you with the Personal Information that you requested or make your requested changes if i) the information is reasonably available; ii) the information does not infringe on the privacy of other individuals, and iii) the disclosure or changing of the information is not otherwise prohibited by law or internal policies or procedures. For requests, we will reasonably describe the types of Personal Information that we generally collect, how it is used, and with whom it is shared.
b. Communications. You may elect to opt-out of e-mail and text communications from us by following the instructions provided in such communications or by contacting us as described in this Privacy Policy. Even after opting out, you may still receive service oriented, non-promotional communications from us and promotional communications from other third-parties as a result of their own interactions or transactions with you. Please allow time for us to process requests. You should contact us should there be any concerns about your opt-out request.
c. Targeted Advertising. You may opt-out from many third-parties who serve online advertising, including some who serve ads on the Progressive Platforms and elsewhere online, by visiting http://www.networkadvertising.org/managing/opt_out.asp; or http://www.aboutads.info/choices/. Opting out does not mean you will not see any ads when using the Progressive Platforms, but the ads that you see will no longer be customized to you based on your profile or interactions with us.
d. “Do-Not-Track.” Your browser settings may allow you to automatically transmit a “Do Not Track” signal to websites and online services that you visit. Like many websites and online services, the Progressive Platforms do not alter their practices when they receive a “Do Not Track” signal from your browser. To find out more about “Do Not Track,” please visit www.allaboutdnt.com.

Progressive Leasing maintains administrative, technical, and physical safeguards intended to protect against the loss, misuse, unauthorized access, and disclosure of information, including your social security number. Although Progressive Leasing takes such precautions seriously, it is impossible for us to guarantee the safety and security of your information. Progressive Leasing’s policies prohibit the unlawful disclosure of personal information. Progressive Leasing shares personal information externally only where federal and state law allows or requires it. Internally, it is Progressive Leasing’s policy to limit the access, use, and disclosure of personal information to be in line with the job dues of Progressive Leasing associates, as well as applicable law. Please note that Progressive Leasing does not warrant the security of any information that is collected, and customers use Progressive Platforms and services, and provide Progressive Leasing with personal information at the customer’s risk.

Processes, Policies and Procedures

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

Physical Security

Progressive Leasing physical security for in-scope systems is managed by both Progressive Leasing and its colocation data center provider, Flexential.

Each facility has a designated reception area which is attended by either a receptionist or a security guard 24 hours per day. Access to the reception area is unlocked from 7am to 5pm on business days and is locked at other times. When locked, a visitor presses a buzzer to attract the attention of the guard at the visitor desk who can release the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.

All remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors present a valid, government-issued photo ID. The visitor’s name, employer, and purpose for visit are recorded in a visitor log and his or her visit is approved by a Progressive Leasing employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Entrances to the colocation data center are restricted by two doors; access through the first door is gained by using a key card to deactivate the locking mechanism, and access through the second door is granted by using a biometric hand reader and personal identification number (PIN). Security software and hardware are maintained by Flexential.

Upon an employee’s termination of employment, the Human Resources system automatically generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then securely given to the physical security department for recording and destruction. On a quarterly basis, secured zone owners review access to their secured zones. Access listings are generated by security and distributed to the zone owners via the event management system. Secured zone owners review the listings and indicate the required changes in the event management record. The record is routed back to the access administrators for processing. The manager of physical security identifies any records not returned within two weeks and follows up with the secured zone owner.

The in-scope systems are hosted by Flexential and AWS; therefore, Flexential and AWS are responsible for implementing physical security controls over the housed in-scope systems. Flexential and AWS are responsible for additional physical security controls. Refer to the Subservice Organization section below for additional information.

Logical Access

Progressive Leasing requires users to be uniquely identified and authenticated to access system resources. Access is restricted based on job roles. Access reviews are completed at least quarterly.

Resources are identified in the configuration management database configuration management database with appropriate owners who are responsible for approving and reviewing access.

Employees authenticate to access Progressive Leasing systems using an Active Directory user ID and password. Onboarding and Offboarding processes are managed through ServiceNow.

Remote network access requires virtual private network (VPN) using multi-factor authentication.

Administrative or privileged access is managed through secondary AD accounts and are reviewed quarterly. Passwords for personal Active Directory accounts are rotated as per policy. Personal database administrative accounts are fully managed by the enterprise password vault and is checked out on an as needed basis using single sign-on with multi-factor authentication.

Computer Operations - Backups

Production data is backed up and monitored by the Infrastructure Systems and Database Administrative team. The Infrastructure Systems team uses Veeam for backup and recovery of virtual machines. The Database Administrative team uses native SQL backups for production databases.

Infrastructure System Engineers or Database Administrators receive notifications for failed backup jobs and resolve issues with the appropriate team.

Backups are stored in the local data center to a backup target, which are then synced to a secondary site. The West Jordan datacenter (SLC) syncs to the Phoenix (PHX) datacenter, and vice-versa. Dedicated links between sites ensure that bandwidth is sufficient for transmission of backups within the backup window.

Some data is backed up externally in Amazon Web Services Simple Storage Service (‘AWS S3’), which is used for longer-term storage.

The in-scope systems are hosted by Flexential; therefore, Flexential is responsible for implementing physical security controls over the housed in-scope systems.

Computer Operations - Availability

Systems and applications are monitored on a 24x7x365 basis. Notifications are sent to ServiceNow Event Management, where the incident is evaluated for severity and criticality and assigned to the appropriate owner. Procedures for handling alerts are documented in the ServiceNow Knowledge Base.

Critical alerts are escalated after hours to on-call personnel in accordance with defined policies.

Progressive Leasing designs for High Availability where possible. Applications run on a redundant server behind application pools or firewalls. Critical databases are hosted in Always On clusters.

Infrastructure teams monitor capacity utilization to ensure that applications are operating properly. Capacity utilization is evaluated over time to ensure that the infrastructure capacity will meet future growth projections. Infrastructure capacity monitoring includes, but is not limited to, the following:

- Data center space, power and cooling
- Storage array capacity and performance
- VM metrics, including memory and central processing unit (CPU)
- Network Bandwidth
- Database capacity and latency

Progressive Leasing has implemented a patch management process for servers across environments in a monthly cycle. Patches are applied first to Dev and QA environments, then to RC (Release Candidate) environment, and ultimately to the Production environment. Patching work is done under a Change ticket and reviewed by the Change Advisory Board (CAB) prior to implementation.

The in-scope systems are hosted by Flexential; therefore, Flexential is responsible for implementing physical security controls over the housed in-scope systems.

Change Control

Progressive Leasing maintains documented Change Control procedures and policies documentation to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements and required approval procedures.

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

Software code repositories are utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to the originating request and developer. Branch permissions and processes are set as a control to prevent undetected and untested changes from reaching the production environment.

Progressive Leasing has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Progressive Leasing system owners review proposed operating system patches to determine whether the patches are applied. CAB processes are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them.

Progressive Leasing's systems staff validates that patches have been installed and if applicable that reboots have been completed.

Data Communications

Progressive Leasing's main database system is built upon a stable supported version of Microsoft SQL Server. Login grants are controlled, monitored, and audited on a quarterly basis and support TLS1.2 or later connections.

All sensitive data is encrypted at a column level at rest using an Advanced Encryption Standard (AES)-256 key and utilize a hash of at least SHA-2 or more secure hashing algorithm.

Data access from applications is authorized through AD authentication. Key employees are granted access through internal network connections only.

Boundaries of the System

The scope of this report includes the Lease to Own Services System performed in the Draper, Utah and Glendale, Arizona facilities.

This report does not include the cloud hosting services provided by AWS at multiple facilities or the data center and cloud operations services provided by Flexential at the Aurora (Denver, Colorado), Englewood (Denver, Colorado), Downtown Salt Lake City, Utah (Delong), Richardson, Texas, Allentown, Pennsylvania, Hillsboro Oregon (Brookwood), Calgary, AB, South Charlotte, North Carolina, Alpharetta and Norcross (Atlanta, Georgia), Downtown Louisville, Kentucky, and Nashville, Tennessee (Cool Springs) locations.

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

Control Environment

Integrity and Ethical Values

All Progressive Leasing employees are expected to demonstrate good judgement, ethical behavior, and common sense. It is the duty and responsibility of every Progressive Leasing employee to be aware of and abide by existing polices and work rules.

People have documented policies and procedures and consults with internal and external legal counsel on a regular basis for matters related to human resources issues.

All Progressive Leasing employees are given access to the online employee resources page (replacing the legacy handbook) available through an intranet site. Contained, are a myriad of contents related to ethics, values, and commitments expected for employment.

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

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

Commitment to Competence

Consistent with industry standard hiring practices, Progressive Leasing's hiring teams diligently work with hiring managers to determine which skills and competencies would best support the role needed on each team. These skills are carefully evaluated by corporate recruiters prior to onsite interviews. Skills and competencies are then carefully assessed by the hiring manager prior to hiring.

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

Progressive Leasing'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.

Executive Management meetings are held weekly to discuss major initiatives and issues that affect the business. Risk, control, and compliance discussions are part of the regularly discussed topics in alignment with one of the key goals to keep compliance and security in the forefront.

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.
- 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

Progressive Leasing's organization structure is built upon a foundation that supports critical business functions and ensures a consistent future of business progression and continuity. This structure is aligned with industry standards and is consistent with any reporting structures and design that is required by regulation.

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

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

Human Resources Policies and Practices

All employees are currently required to adhere to and agree to a set of policies prior to beginning employment. The following policies and information are reviewed as part of the onboarding process:

- Acceptable use policy
- Access control policy
- Attendance and punctuality
- Clean desk policy
- Conduct policy
- Dress Code
- Drug Test Policy and Process
- Harassment Policy
- Introductory Period/Equal Employment Opportunity Statement/At Will Employment Policy
- Paid Time Off Policy
- Referral Bonus Policy
- Tuition Reimbursement Policy

In addition to these policies required at onboarding, employees are also required to annually review and adhere to a number of other policies. Policies accepted include (but are not limited to) critical compliance and security policies.

Employees are also required to complete companywide trainings on an annual basis. These trainings can include (But are not limited to):

- At-Will Employment Acknowledgment
- Bring Your Own Device to Work (BYOD) Policy Acknowledgement
- Code of Conduct
- Compliance Manual: Account Security
- Compliance Manual: External Relationships
- Compliance Manual: Leasing
- Compliance Manual: Processes (15 min)
- Compliance: Collections 2019
- Compliance: Overall Compliance 2019
- Preventing Unlawful Workplace Harassment: Employee Edition
- Retailer Procedures
- Bring Your Own Device to Work (BYOD) Policy Acknowledgement
- Code of Conduct
- Compliance Manual: Account Security
- Compliance Manual: External Relationships
- Compliance Manual: Leasing
- Compliance Manual: Processes (15 min)
- Compliance: Collections
- Compliance: Overall Compliance
- Phishing Security Training

- Preventing Unlawful Workplace Harassment: Employee Edition
- Retailer Procedures
- ServiceNow Training for Users
- The Top 10 Security Awareness Fundamentals

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

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

Risk Assessment Process

Risk assessment and corresponding processes live throughout the organization and align with enterprise risk strategies and requirements. Company compliance and risk programs are designed to prevent and detect violations of applicable law, industry best practice, company risk tolerance levels, or company Code of Business Conduct and Ethics.

Risk assessment activities are used to identify, estimate, and prioritize risks to Progressive Leasing and its assets. Risk assessments include identification of impact, likelihood, inherent risk, control existence/effectiveness, and residual risk. Residual risks which are most impactful to the organization are reviewed to determine a course of action for risk treatment, as appropriate.

Security Risk Assessments

Security risk activities are not only supported by internal business strategy but are built upon the foundation of industry best practices and supporting frameworks. Progressive Leasing subscribes to many frameworks which require robust risk assessment requirements to be met. These frameworks and standards include: PCI-DSS, SOC2 service organization controls (Type 2, 5 Trust Services Criteria), ISO27001 controls, and the NIST cyber security framework. Risk decisions and mitigating activities are also supported by a strong set of internal controls which are validated on a regular basis. Controls are continually validated internally, and a majority of controls are validated for effectiveness at least annually by third-parties.

The environment in which the system operates; the commitments, agreements, and responsibilities of Progressive Leasing's Lease to Own Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. Progressive Leasing 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, Progressive Leasing's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Risk and Control Self-Assessments

The Risk and Control Self-Assessment program (RCSA) enables business unit management and process owners to identify, understand, assess, measure, manage and monitor material risks and controls. The objectives of an RCSA are to identify inherent and residual risk in business processes and to determine whether the control environment of a given business unit or activity is adequate and effective.

Integration with Risk Assessments

Enterprise Risk Management (ERM) has developed tools and methodologies to enable consistency in risk identification and assessment across the organization. These tools and methodologies are being implemented in a phased approach across the organization.

Information and Communications Systems

Information and communication are an integral part of the internal control system at Progressive Leasing. At Progressive Leasing, information is identified, captured, processed, and reported by various information systems, as well as through conversations with merchants, vendors, regulators, and employees.

Various weekly meetings are held to discuss operational efficiencies within the applicable areas. These messages are then communicated to the organization (i.e. town halls, department meetings, team meetings, executive meetings) and in written form (i.e. policies and procedures). General updates to entity-wide security policies and procedures are usually communicated to the appropriate personnel via e-mail messages.

Specific information systems used to support Progressive Leasing's Lease to Own Services System are described in the Description of Services section above.

Monitoring Controls

Many Progressive Leasing teams are involved in the monitoring of company controls. The Compliance department has a testing and monitoring program in place to verify Progressive Leasing and Progressive Leasing retailer partners are following the policies and procedures. Compliance management does a quarterly review of information obtained through the monitoring program to ensure the proper controls are in place and to recommend enhancements as needed. Compliance also has a team of analysts who follow a testing calendar to verify the company is following policies and procedures. Each month management will review the findings of the analysts. Any recommended enhancements or corrections are sent to the appropriate teams.

The Compliance team utilizes field examiners who perform in-store visits to verify retailer adherence to policies and procedures. A team of compliance analysts also use an internal tracking tool of customer complaints to review company data pertaining to Progressive Leasing retail partners. Compliance sends corrective actions for Progressive Leasing retailer partners in the form of a case via the Sales team as necessary. Any escalated issues follow appropriate procedures and are reviewed by management. Deviations, cases, and escalated issues are tracked in internal systems.

Progressive Leasing's technology compliance team is organized under the security department and is constantly testing and validating the effectiveness of controls which relate to security requirements. Security requirements stem from security standards, frameworks, law, contracts, and industry best practices. These controls are meticulously managed by this team, evaluated for effectiveness, and constantly improved. Any significant deficiencies or deviations are reported to management for proper reporting and handling. Most of these controls are also externally validated by third-parties for effectiveness at least annually.

Progressive Leasing also employs a financial controls team which ensures adequate design of internal controls over financial reporting for SOX (Sarbanes-Oxley) purposes. Key SOX controls are evaluated at least annually by a third-party to evaluate operating effectiveness. Any design or operating deficiencies are evaluated and reported to management for proper disclosure, in accordance with SOX requirements.

On-Going Monitoring

Progressive Leasing'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 Progressive Leasing'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 Progressive Leasing'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.

Changes to the System Since the Last Review

Migrated cardholder data environment (CDE) to AWS cloud.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, Processing Integrity, Confidentiality and Privacy criterion were applicable to the Progressive Leasing Lease to Own Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities, or the data center and cloud operations services provided by Flexential at the Aurora (Denver, Colorado), Englewood (Denver, Colorado), Downtown Salt Lake City, Utah (Delong), Richardson, Texas, Allentown, Pennsylvania, Hillsboro Oregon (Brookwood), Calgary, AB, South Charlotte, North Carolina, Alpharetta and Norcross (Atlanta, Georgia), Downtown Louisville, Kentucky, and Nashville, Tennessee (Cool Springs) locations.

Subservice Description of Services

The AWS S3 cloud hosting services are used for longer term storage.

Flexential's data center and cloud operations services are used to host and support various functionalities within Progressive Leasing.

Complementary Subservice Organization Controls

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

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4 CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		Objects are stored redundantly across multiple fault-isolated facilities.
		The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Subservice Organization - Flexential		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4 CC7.2	Two separate multi-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 entrances
		Visitors are required to sign-in with onsite security personnel prior to entering 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 wear a visitor badge while visiting the data centers.
		Client equipment is maintained in lockable cages or racks within the data centers.
		There are no exterior facing windows in the walls of the areas where client production servers are located.
		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
		Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.
		The Director of Compliance reviews user account access of terminated employees on a quarterly basis.
		A termination checklist is completed and access is revoked for employees as a component of the employee termination process.
Availability	A1.2	Documented policies and procedures are in place to govern environmental security practices and responses to certain environmental security events.

Subservice Organization - Flexential		
Category	**Criteria**	**Control**
		The data centers are protected by the following fire detection and suppression controls: • Audible and visual fire alarms • Pre-action dry-pipe water sprinklers and/or agent-based fire suppression system • Fire and smoke detectors • Hand-held fire extinguishers
		Management obtains inspection reports to ensure that third-party specialists inspect the fire detection and suppression systems on an annual basis.
		The data centers are equipped with multiple air conditioning units to regulate temperature and humidity.
		Management obtains inspection reports to ensure that third-party specialists inspect the air conditioning units on a quarterly basis.
		The data centers are equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak.
		The data centers are connected to multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage.
		Management obtains inspection reports and/or invoices to ensure that third-party specialists inspect the UPS systems on a quarterly basis.
		The data centers are equipped with fueled electric power generators to provide backup power in the event of a power outage.
		Management contracts with third-party specialists to inspect the fueled electric power generators on a quarterly basis and the inspection report is retained as evidence of completion.
		Management obtains inspection reports to ensure that generators are load tested on a quarterly basis.
		Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including, but not limited to, the following: • Fire alarm status and suppression systems • Temperature • Humidity and air quality • Power levels and availability
		The environmental monitoring application is configured to notify operations personnel via on-screen and/or e-mail alert notifications if certain predefined thresholds are exceeded on monitored systems.
		For subscribing customers, an automated backup system is in place to perform scheduled backups of customer systems according to a predefined schedule.
		The automated backup system is configured to perform daily incremental and weekly full backups of managed services infrastructure.

Subservice Organization - Flexential		
Category	**Criteria**	**Control**
		Backup system status notifications are available for subscribing customers through the web portal.
		For subscribing customers, disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

Progressive Leasing management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, Progressive Leasing performs monitoring of the subservice organization controls, including the following procedures:

- Holding discussions with vendors and subservice organizations
- Making regular site visits to vendor and subservice organizations' facilities
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

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

Availability

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

Processing Integrity

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

Confidentiality

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

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

Privacy

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

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

The privacy criteria are organized as follows:

i. Notice and communication of objectives. The entity provides notice to data subjects about its objectives related to privacy.

ii. Choice and consent. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

iii. Collection. The entity collects personal information to meet its objectives related to privacy.

iv. Use, retention, and disposal. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.

v. Access. The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

vi. Disclosure and notification. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

vii. Quality. The entity collects and maintains accurate, up-to date, complete, and relevant personal information to meet its objectives related to privacy.

viii. Monitoring and enforcement. The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Control Activities Specified by the Service Organization

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

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

SECTION 4

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

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

A-LIGN ASSURANCE's examination of the controls of Prog Leasing was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Prog Leasing and did not encompass all aspects of Prog Leasing'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, procedures and the code of conduct.	Inspected the code of conduct and the entity's SharePoint to determine that core values were communicated from executive management to personnel through policies, procedures and the code of conduct.	No exceptions noted.
		A code of conduct is documented to communicate workforce conduct standards and enforcement procedures.	Inspected the training material to determine that a code of conduct was documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the code of conduct.	Inquired of the Chief Legal and Compliance Officer regarding acknowledgment of code of conduct to determine that upon hire, personnel were required to acknowledge the code of conduct.	No exceptions noted.
			Inspected the code of conduct to determine that upon hire, personnel were required to acknowledge the code of conduct.	No exceptions noted.
			Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge code of conduct.	Testing of the control activity disclosed that the code of conduct was not acknowledged for 3 of 25 new hires sampled.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
		Personnel are required to acknowledge the code of conduct on an annual basis.	Inspected the signed code of conduct acknowledgement 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 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 sanction policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Observed an employee call the anonymous hotline number to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the anonymous hotline number on the employee's login interface and entity's website to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the code of conduct slide deck and entity's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Upon hire, personnel are required to sign a non-disclosure agreement.	Inspected the signed non-disclosure agreement for a sample of new hires to determine that upon hire, personnel were required to sign a non-disclosure agreement.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the 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 roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions for a sample of executive member job roles and including revision dates to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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 form 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 implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually.	Inspected the performance 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 implemented 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 completed internal controls matrix and Information Security Risk Committee meeting's slide deck to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented 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 implemented 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 implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	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.	Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
		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.	Inspected the job description for a sample of job roles 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.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	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, the completed internal controls matrix, and job description for a sample of job roles 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 the job description for a sample of job roles 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 Third-Party Management Standard and 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.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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.	Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the 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.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the Third-Party Management Standard and 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.
		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**
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the interview questionnaire for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		The entity evaluates the competencies and experience of third-parties prior to working with them.	Inspected the vendor risk assessment for a sample of third-parties to determine that the entity evaluated the competencies and experience of third-parties prior to working with them.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the job description for a sample of job roles and job application 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.
		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 recruiting policies and procedures and staffing and recruiting service agreement 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.

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 works with an outside vendor to attract individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the third-party agreement to determine that the entity worked with an outside vendor to attract individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the Continued Professional Education (CPE) training tracker for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training program to determine that executive management created a training program for its employees.	No exceptions noted.
		Executive management uses an outside vendor to assist with its continued training of employees.	Inspected the training material to determine that executive management used an outside vendor to assist with its continued training of employees.	No exceptions noted.
		The entity has implemented a mentor program to develop its personnel.	Inspected the mentor program to determine that the entity created a mentor program for its employees.	No exceptions noted.
		Executive management tracks and monitors compliance with CPE training requirements.	Inspected the CPE training tracker to determine that executive management tracked and monitored compliance with CPE training requirements.	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**
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet 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 and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the training assessment to determine that the entity assessed the training needs on an annual basis.	No exceptions noted.
		As part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trains its personnel.	Inspected the training materials to determine that as part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trained its personnel.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upon hire, personnel are required to acknowledge the code of conduct.	Inquired of the Chief Legal and Compliance Officer regarding acknowledgment of code of conduct to determine that upon hire, personnel were required to acknowledge the code of conduct.	No exceptions noted.
			Inspected the code of conduct to determine that upon hire, personnel were required to acknowledge the code of conduct.	No exceptions noted.
			Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge code of conduct.	Testing of the control activity disclosed that the code of conduct was not acknowledged for 3 of 25 new hires sampled.
		Personnel are required to acknowledge the code of conduct on an annual basis.	Inspected the signed code of conduct acknowledgement 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 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 sanction policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint.	Inspected the job description for a sample of job roles 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.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	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**
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet 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 and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that executive management established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	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 and made available to personnel through the entity's SharePoint.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired the Senior Software Engineer regarding edit checks to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Observed the input of information into the in-scope system to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Inspected the edit check configurations 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 data flow diagram and information security policy 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.

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 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, IPS configurations, encryption methods and configurations and VPN authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data and information critical to the system is assessed annually for relevance and use.	Inspected the database activity log to determine that data and information critical to the system was assessed annually for relevance and use.	No exceptions noted.
		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.	Core values are communicated from executive management to personnel through policies, procedures and the code of conduct.	Inspected the code of conduct and the entity's SharePoint to determine that core values were communicated from executive management to personnel through policies, procedures and the code of conduct.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the code of conduct.	Inquired of the Chief Legal and Compliance Officer regarding acknowledgment of code of conduct to determine that upon hire, personnel were required to acknowledge the code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the code of conduct to determine that upon hire, personnel were required to acknowledge the code of conduct.	No exceptions noted.
			Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge code of conduct.	Testing of the control activity disclosed that the code of conduct was not acknowledged for 3 of 25 new hires sampled.
		Personnel are required to acknowledge the code of conduct on an annual basis.	Inspected the signed code of conduct acknowledgement 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.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Observed an employee call the anonymous hotline number to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the anonymous hotline number on the employee's login interface and entity's website to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the code of conduct slide deck and entity's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint.	Inspected the job description for a sample of job roles 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.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the CPE training tracker for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint.	No exceptions noted.
		The entity's policies and procedures, code of conduct are made available to personnel through the entity's SharePoint.	Observed the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's SharePoint to determine that the entity's policies and procedures, code of conduct were made available to personnel through the entity's SharePoint.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training completion form for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training completion tracking tool for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the Cybersecurity power point deck 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.
		Changes to job roles and responsibilities are communicated to personnel through the entity's SharePoint.	Inspected the entity's SharePoint to determine that changes to job roles and responsibilities were communicated to personnel through the entity's SharePoint.	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 system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's SharePoint.	Inspected the incident response policies and procedures and the entity's SharePoint to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's SharePoint.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's SharePoint.	Inspected the entity's SharePoint to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's SharePoint.	No exceptions noted.
		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 information security policies and procedures to determine that the information security policies and procedures that communicated the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	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 incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that 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.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Observed an employee call the anonymous hotline number to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the anonymous hotline number on the employee's login interface and entity's website to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the code of conduct slide deck and entity's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's SharePoint.	Inspected the incident response policies and procedures and the entity's SharePoint to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's SharePoint.	No exceptions noted.
		The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity's master customer agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the master customer agreement to determine that the entity's master customer agreement outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the customer 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 updated agreements.	Inspected the entity's updated agreement to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers via updated agreements, website notices, or mass notifications.	No exceptions noted.
		Executive management meets annually with operational management to discuss the results of assessments performed by third-parties.	Inspected the Cybersecurity KPI slide deck to determine that executive management met annually with operational management to discuss the results of assessments performed by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the master third-party agreement to determine that the entity communicated to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	No exceptions noted.
		Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers via updated agreements.	Inspected the entity's intranet and updated agreement to determine that changes to commitments and requirements relating to confidentiality were communicated to third-parties, external users and customers via updated agreements.	No exceptions noted.
		The entity communicates to external users, vendors and service providers the system commitments and requirements relating to privacy through the use of third-party agreements.	Inspected the third-party master agreement to determine that the entity communicated to external users, vendors and service providers the system commitments and requirements relating to privacy through the use of third-party agreements.	No exceptions noted.
		Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers via website notices.	Inspected the entity’s website to determine that changes to commitments and requirements relating to confidentiality were communicated to third-parties, external users and customers via website notices.	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 incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that 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.

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.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		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.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint.	No exceptions noted.
		The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, Annual Performance Manager Evaluation 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.

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 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 policy and 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 a quarterly basis.	Inspected the cybersecurity slide deck for a sample of quarters to determine that executive management reviewed policies, procedures and other control documents for alignment to the entity's objectives on a quarterly basis.	No exceptions noted.
		Executive management reviews and addresses repeated control failures.	Inspected the Cybersecurity Townhall slide deck for a sample of quarters to determine that executive management reviewed and addressed repeated control failures.	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 documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer 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 documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the Annual Performance Manager Evaluation, 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.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the Cybersecurity Review slide deck to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls framework is based on a recognized framework.	Inspected the compliance reports to determine that the entity's internal controls framework was based on a recognized framework.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the completed internal controls matrix and the information security program standard to determine that the entity's internal control environment took into consideration affecting laws, regulations, standards, and legislatures.	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.
		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 policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 policy and 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.
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.	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the Third-Party Management Standard and 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.
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment and management policy to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk assessment and management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.

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**
		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.
		The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	Inspected the risk assessment and management policy and the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policy and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment and management policy and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	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 policy and 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.

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
		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 policy and the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policy and 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 policy and 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.

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 obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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 policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed fraud 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**
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed fraud assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		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 fraud 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 fraud 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 fraud 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the Third-Party Management Standard and 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.
		Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policy and the completed risk assessment to determine that changes to the regulatory, economic and physical environment in which the entity operates were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		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 policy and 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.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Risk Assessment</th></tr>
<tr><th>CC3.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.</td><td>Inspected the risk assessment and management policy and 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.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.</td><td>Inspected the risk assessment and management policy and 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.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.</td><td>Inspected the risk assessment and management policy and 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.</td><td>No exceptions noted.</td></tr>
</table>

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 obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the 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 meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the Third-Party Management Standard and 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.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint.	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**
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	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.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures and management meeting minutes to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	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
		On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the Cybersecurity Townhall slide deck to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		A data backup restoration test is performed on a weekly basis.	Inquired of the Senior Security Analyst regarding restoration testing to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.
			Inspected the completed backup restoration test for a sample of weeks to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.
		Internal and external vulnerability scans are performed monthly and remedial actions are taken where necessary.	Inquired of the Director, Information Security regarding vulnerability scanning to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the vulnerability scanning policies and procedures to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	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 completed vulnerability scan results for a sample of months and the supporting ticket for a sample of critical vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	Testing of the control activity disclosed that remedial actions were not taken timely for 25 of 25 critical vulnerabilities identified.
		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
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		Logical access reviews are performed quarterly.	Inquired of the Director, Financial Controls regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert generated from the monitoring software 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				
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.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	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 policy and 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.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policy and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the Cybersecurity slide deck 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 Cybersecurity slide deck 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 failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Inquired of the Director, Information Security regarding vulnerabilities, deviations, and control failures/gaps to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the Information Security Program Standard and Endpoint Vulnerability Management Standard to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment 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
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed no deviations occurred during the review period.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps to determine that control failures/gaps identified from the various assessments performed on the environment 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 failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inquired of the Director, Information Security regarding vulnerabilities, deviations, and control failures/gaps to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the Information Security Program Standard and Endpoint Vulnerability Management Standard to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated and addressed.	No exceptions noted.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the various assessments performed on the environment were documented, investigated and addressed.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely. Testing of the control activity disclosed that no deviations occurred during the review period.

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 various assessments performed on the environment and supporting incident tickets for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that deviations identified from the various assessments performed on the environment were documented, investigated and addressed.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely. Testing of the control activity disclosed that no deviations occurred during the review period.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps to determine that control failures/gaps identified from the various assessments performed on the environment were documented, investigated and addressed.	No exceptions noted.
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions.	Inquired of the Director, Information Security regarding vulnerabilities, deviations, and control failures/gaps to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment 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 Information Security Program Standard and Endpoint Vulnerability Management Standard to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely. Testing of the control activity disclosed that no deviations occurred during the review period.

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 various assessments performed on the environment and supporting incident tickets for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that deviations identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely. Testing of the control activity disclosed that no deviations occurred during the review period.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps to determine that control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the Cybersecurity Townhall slide deck to determine that management tracked whether vulnerabilities, deviations and control failures/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.	Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	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 policy and 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.

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 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 failures/gaps identified as part of the various evaluations performed.	Inquired of the Director, Information Security regarding vulnerabilities, deviations and control failures/gaps to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the entity's risk management and monitoring tool 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
			Inspected the supporting incident ticket for an internal control that had failed to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the completed 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 completed internal controls matrix to determine that prior to the development and implementation of internal controls into the environment, management considers 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 completed internal controls matrix to determine that 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 completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		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.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has documented the 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 completed 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.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the completed 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 completed 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**
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.	The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	Inspected the completed 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 • 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 completed internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Information Security Risk Committee's slide deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint.	Inspected the job description for a sample of job roles 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.	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 personnel through the entity's SharePoint.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and chief legal and compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the completed 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.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the completed 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 completed 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.
		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 procedures and the completed 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.

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**
		Process owners and management investigate and troubleshoot control failures.	Inquired of the Senior Security Analyst regarding control failures to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the completed risk assessment to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
		The effectiveness of the internal controls implemented within the environment is evaluated annually.	Inspected the cybersecurity townhall slide deck to determine that the effectiveness of the internal controls implemented within the environment was 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 that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Director, Information Security regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Network user access is restricted via role based security privileges defined within the access control system.	Inquired of the Director, Information Security regarding network access 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**
			Inspected the network user listing and access rights to determine that network user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to authorized personnel.	Inquired of the Director, Information Security regarding administrative access to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Network users are authenticated via individually-assigned user accounts and passwords.	Inquired of the Director, Information Security regarding network authentication to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to the network to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the password settings to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The network is configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit 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 changes • Privilege use • Process tracking • System events	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 logs are maintained for review when needed.	Inquired of the Director, Information Security regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
		Production server user access is restricted via role based security privileges defined within the access control system.	Inquired of the Senior Systems Engineer regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production server user listing and access role to determine that production server user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Production server administrative access is restricted to authorized personnel.	Inquired of the Senior Systems Engineer regarding administrative access to determine that production server administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production server administrator listing and access roles to determine that production servers administrative access 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
		Production server users authenticate via Okta into CyberArk to obtain RDP password credentials to authenticate into the production server.	Inspected the Group Policy password configurations to determine that production server users authenticate via Okta into CyberArk to obtain RDP password credentials to authenticate into the production server.	No exceptions noted.
		Production servers are configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the Group Policy password configurations for production servers to determine that the production servers were configured to enforce password requirements that included: • Password history • Minimum password age • Password length • Complexity	No exceptions noted.
		Production server account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Group Policy account lockout configurations for production servers to determine that production server account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	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**
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the audit logging configurations for production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Production server audit logs are maintained for review when needed.	Inquired of the Senior Systems Engineer regarding production server audit logs to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the production server audit log settings and an example audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Production database user access is restricted via role based security privileges defined within the access control system.	Inquired of the Senior Manager, Analytics Engineering regarding production database access to determine that production databases 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**
			Inspected the user listing and access roles for production databases to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production database administrative access is restricted to authorized personnel.	Inquired of the Senior Manager, Analytics Engineering regarding administrative access to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production database administrator listing and access roles to determine that production databases administrative access was restricted to authorized personnel.	No exceptions noted.
		Production database users are authenticated via individually-assigned user accounts and passwords.	Inspected the production database user listings and password configurations for production databases to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production databases are configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the Group Policy password configurations for production databases to determine that production databases were configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Group Policy account lockout configurations for production databases to determine that operating system account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production database audit logging configurations are in place to log user activity and system events.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	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**
		Production database audit logs are maintained for review when needed.	Inquired of the Senior Manager, Analytics Engineering regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.
		Production application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Systems Engineer regarding production application access to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production application user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production application administrative access is restricted to authorized personnel.	Inquired of the Senior Systems Engineer regarding administrative access to determine that production application administrative access 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**
			Inspected the production application administrator listing and access roles to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
		Production application users are authenticated via individually-assigned user accounts and passwords.	Inspected the production application user listing and password configurations to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		The production application is configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the Group Policy password configurations to determine that applications were configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
		Production application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	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
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and a production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained for review when needed.	Inquired of the Senior Systems Engineer regarding application audit logs to determine that application audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the production application audit log extract to determine that production application audit logs were maintained for review when needed.	No exceptions noted.
		VPN user access is restricted via role based security privileges defined within the access control system.	Inquired of the Director, Information Security regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN user listing and access rights to determine that VPN 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**
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Director, Information Security regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inquired of the Director, Information Security regarding remote access to the environment to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment.	No exceptions noted.
			Observed a user access the in-scope environment remotely to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment.	No exceptions noted.
			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.

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 entity’s network architecture diagram 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, an IDS, and an IPS.	Inspected the IDS and IPS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls, an IDS, and an IPS.	No exceptions noted.
		A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the Advanced Encryption Standard (AES).	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	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**
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the Senior Manager, Analytics Engineering regarding the encryption keys to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
			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 are performed quarterly.	Inquired of the Director, Financial Controls regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	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, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Director, Information Security regarding the termination process to determine that logical access to systems was revoked 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**
			Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Director, Information Security regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Director, Information Security regarding privileged access to determine that privileged access to sensitive resources 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
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed quarterly.	Inquired of the Director, Financial Controls regarding user access reviews to determine that logical access reviews were performed quarterly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	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, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Director, Information Security regarding the termination process to determine that logical access to systems was revoked 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**
			Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Director, Information Security regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts 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 policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Director, Information Security regarding privileged access to determine that privileged access to sensitive resources 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
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Network user access is restricted via role based security privileges defined within the access control system.	Inquired of the Director, Information Security regarding network access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			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.
		Production server user access is restricted via role based security privileges defined within the access control system.	Inquired of the Senior Systems Engineer regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production server user listing and access role to determine that production server 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**
		Production database user access is restricted via role based security privileges defined within the access control system.	Inquired of the Senior Manager, Analytics Engineering regarding production database access to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the user listing and access roles for production databases to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Systems Engineer regarding production application access to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production application user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Logical access reviews are performed quarterly.	Inquired of the Director, Financial Controls regarding user access reviews to determine that logical access reviews were performed quarterly.	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 completed access review for the in-scope systems for a sample of quarters to determine that logical access reviews were performed quarterly.	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, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Director, Information Security regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Director, Information Security regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts 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**
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		The entity purges data stored on backups when no longer needed.	Inspected the Record Retention Standard within the entity's information security policy to determine that the entity purged data stored on backups when no longer needed.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the Record Retention Standard and destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	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**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN user access is restricted via role based security privileges defined within the access control system.	Inquired of the Director, Information Security regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inquired of the Director, Information Security regarding remote access to the environment to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment.	No exceptions noted.
			Observed a user access the in-scope environment remotely to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment.	No exceptions noted.
			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.

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**
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Network address translation (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, TLS, and digital certificates are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, TLS, and digital certificates were used for defined points of connectivity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Director, Information Security regarding remote connectivity to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Manager, Analytics Engineering regarding access to stored data to determine that logical access to stored 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**
			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 and firewall rule sets for production servers 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 and firewall rule sets for production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram, IDS, and IPS configurations to determine that an IDS and an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		IDS and IPS logs are maintained and reviewed.	Inspected the IDS and configurations and an example IDS and IPS log extract to determine that IDS and IPS logs were maintained and reviewed.	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
		Antivirus software is installed on workstations and servers 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 and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations on a continuous basis.	Inspected the centralized antivirus configurations to determine that the antivirus software was configured to scan workstations on a continuous basis.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inquired of the Director, Information Security regarding remote access to the environment to determine that users authenticated via multi-factor authentication prior to being granted remote access to the 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**
			Observed a user access the in-scope environment remotely to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment.	No exceptions noted.
			Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	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**
		VPN, TLS, and digital certificates are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, TLS, and digital certificates were used for defined points of connectivity.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Director, Information Security regarding remote connectivity to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Manager, Analytics Engineering regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rule sets for production servers 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 and firewall rule sets for production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram, IDS, and IPS configurations to determine that an IDS and an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		IDS and IPS logs are maintained and reviewed.	Inspected the IDS and configurations and an example IDS and IPS log extract to determine that IDS and IPS logs were maintained and reviewed.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
		System data is encrypted during the replication process between cloud environments.	Inspected the backup replication configurations to determine that system data was replicated and encrypted via the cloud in real-time.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Senior Manager, Analytics Engineering 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 listing of users with the ability to recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated offsite by a third-party vendor in real time.	Inspected the contract with the offsite backup storage vendor to determine that backup media was replicated offsite by a third-party vendor in real time.	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
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Backups are stored in an encrypted format.	Inspected the backup configurations and an example backup log extract to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Production data is backed up and replicated to an offsite facility in real-time.	Inspected the backup replication configurations to determine that production data was backed up and replicated to an offsite facility real-time.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Antivirus software is installed on workstations and servers 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 and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations on a continuous basis.	Inspected the centralized antivirus configurations to determine that the antivirus software was configured to scan workstations on a continuous basis.	No exceptions noted.
		The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the Director, Information Security regarding the applications and software to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.
			Inspected the denial notification to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Senior Manager, Analytics Engineering regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		FIM software logs are maintained and reviewed.	Inspected the FIM configurations and an example FIM software log extract to determine that FIM software logs were maintained and reviewed.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management 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 monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert generated from the monitoring software 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**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Internal and external vulnerability scans are performed monthly and remedial actions are taken where necessary.	Inquired of the Director, Information Security regarding vulnerability scanning to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the vulnerability scanning policies and procedures to determine that internal and external vulnerability scans were performed monthly 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**
			Inspected the completed vulnerability scan results for a sample of months and the supporting ticket for a sample of critical vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	Testing of the control activity disclosed that remedial actions were not taken timely for 25 of 25 critical vulnerabilities identified.
		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 firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rule sets for production servers 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 and firewall rule sets for production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram, IDS, and IPS configurations to determine that an IDS and an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		IDS and IPS logs are maintained and reviewed.	Inspected the IDS and configurations and an example IDS and IPS log extract to determine that IDS and IPS logs were maintained and reviewed.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		FIM software logs are maintained and reviewed.	Inspected the FIM configurations and an example FIM software log extract to determine that FIM software logs were maintained and reviewed.	No exceptions noted.
		Management defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert generated from the monitoring software to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	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 management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit 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 changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the Director, Information Security regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the network audit log extract to determine that network audit logs were maintained for review when 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
		Production server account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Group Policy account lockout configurations for production servers to determine that production server account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the audit logging configurations for production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Production server audit logs are maintained for review when needed.	Inquired of the Senior Systems Engineer regarding production server audit logs to determine that production server audit logs were maintained for review when 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
			Inspected the production server audit log settings and an example audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the Group Policy account lockout configurations for production databases to determine that operating system account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production database audit logging configurations are in place to log user activity and system events.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production database audit logs are maintained for review when needed.	Inquired of the Senior Manager, Analytics Engineering regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when 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**
			Inspected the production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.
		Production application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and a production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained for review when needed.	Inquired of the Senior Systems Engineer regarding application audit logs to determine that application audit logs were maintained for review when 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**
			Inspected the production application audit log extract to determine that production application audit logs were maintained for review when needed.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rule sets for production servers 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 and firewall rule sets for production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram, IDS, and IPS configurations to determine that an IDS and an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		IDS and IPS logs are maintained and reviewed.	Inspected the IDS and configurations and an example IDS and IPS log extract to determine that IDS and IPS logs were maintained and reviewed.	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 and servers 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 and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations on a continuous basis.	Inspected the centralized antivirus configurations to determine that the antivirus software was configured to scan workstations on a continuous basis.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within 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**
		FIM software logs are maintained and reviewed.	Inspected the FIM configurations and an example FIM software log extract to determine that FIM software logs were maintained and reviewed.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert generated from the monitoring software to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	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 management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that 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.

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**
		Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the cybersecurity slide deck to determine that management reviewed reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that 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 policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and 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 is documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	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 that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Director, Information Security regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the Security Incident Policy to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Director, Information Security regarding critical incidents to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	No exceptions noted.
			Inspected the Security Incident Policy to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the notice letter for an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		Identified incidents are evaluated to determine whether: • They resulted in the unauthorized disclosure or use of personal information • There has been a failure to comply with applicable laws or regulations	Inspected the Security Incident Policy to determine that identified incidents were evaluated to determine whether: • They resulted in the unauthorized disclosure or use of personal information • There has been a failure to comply with applicable laws or regulations	No exceptions noted.
		Notification is provided to the affected parties when an identified incident results in the unauthorized disclosure or use of personal information.	Inspected the Security Incident Policy to determine that notification was provided to the affected parties when an identified incident resulted in the unauthorized disclosure or use of personal information.	No exceptions noted.
		The affected information is identified when an identified incident results in the unauthorized disclosure or use of personal information.	Inspected the Security Incident Policy to determine that the affected information was identified when an identified incident resulted in the unauthorized disclosure or use of personal information.	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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that 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.
		Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the cybersecurity slide deck to determine that management reviewed reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and 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 policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	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 is documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	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 that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Director, Information Security regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the Security Incident Policy to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and 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.
		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 that 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 policies and 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.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through incident tickets and related communications.	Inquired of the Director, Information Security regarding critical security incidents to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through incident tickets and related communications.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the Security Incident Policy to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through incident tickets and related communications.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through incident tickets and related communications.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		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 that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		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 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.

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 that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.	Inquired of the Director, Information Security regarding critical incidents to determine that to determine that incidents that resulted in unauthorized use or disclosure of personal information were communicated to the data subjects, legal and regulatory authorities, and others as required.	No exceptions noted.
			Inspected the Privacy Policy to determine that incidents that resulted in unauthorized use or disclosure of personal information were communicated to the data subjects, legal and regulatory authorities, and others as required.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents that resulted in unauthorized use or disclosure of personal information were communicated to the data subjects, legal and regulatory authorities, and others as required.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The conduct of individuals and organizations involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.	Inspected the Operations Performance Corrective Action Policy and Privacy Policy to determine that the conduct of individuals and organizations involved in the unauthorized use or disclosure of personal information was evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A data backup restoration test is performed on a weekly basis.	Inquired of the Senior Security Analyst regarding restoration testing to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.
			Inspected the completed backup restoration test for a sample of weeks to determine that a data backup restoration test was performed on a weekly basis.	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				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the cybersecurity slide deck to determine that management reviewed reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Director, Information Security regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the Security Incident Policy to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		Change management requests are opened for incidents that require permanent fixes.	Inspected the Secure Configuration Management Standard 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: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures, and the system build guides for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		A business continuity and disaster recovery plan is 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.

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 business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans and completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Senior Manager, Analytics Engineering regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		FIM software logs are maintained and reviewed.	Inspected the FIM configurations and an example FIM software log extract to determine that FIM software logs were maintained and reviewed.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The change management process has defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • 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 change tickets e-mails to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system changes were authorized and approved by management prior to implementation.	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**
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software settings 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.
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		System patches/security updates are performed on a configured schedule.	Inspected the system patching configurations and an example patching job for a sample of weeks to determine that system patches were performed on a configured schedule.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the development, QA and production servers 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 ticket for a sample of infrastructure, operating system, database and application 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
		Back out procedures are documented to allow for rollback of application changes when changes impaired system operations.	Inspected the rollback procedures to determine that back out procedures were documented to allow for rollback of application changes when changes impaired system operation.	No exceptions noted.
		A code review is systematically required prior to deploying the PR into the production environment.	Inspected the supporting change ticket for a sample of infrastructure, database and application changes to determine that a code review was systematically required prior to deploying the PR into the production environment.	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 ticket for a sample of infrastructure, operating system, database and application changes to determine that system changes were tested prior to implementation, and that types of testing performed depended on the nature of the change.	No exceptions noted.
		System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policies and procedures and supporting change ticket for a sample of incidents to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management 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.
		The entity creates test data that replaces confidential information with test information during the change management process.	Inspected a set of fictitious data used during development activities to determine that the entity created test data that replaced confidential information with test information during the change management process.	No exceptions noted.
		Data owners approve any storage or use of production, confidential information in non-production environments.	Inspected the change tickets to determine that data owners approved the storage or use of production, confidential information in non-production environments.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity creates test data using data masking software that replaces personal information with test information during the change management process.	Inspected the data masking software and a set of fictitious data used during development activities to determine that the entity created test data using data masking software that replaced personal information with test information during the change management 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**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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 policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policy and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment and management policy and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	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 risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policy and 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.
		Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities.	Inspected the risk assessment and management policy to determine that documented policies and procedures were in place to guide personnel in performing risk assessment and risk mitigation activities.	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.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the Third-Party Management Standard and the completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the Third-Party Management Standard and 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.
		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 policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policy and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	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.
		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 Third-Party Management Standard 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 Third-Party Management Standard and 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 Third-Party Management Standard and the completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the Third-Party Management Standard 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 Chief Legal and Compliance Officer 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.
		Management has established exception handling procedures for services provided by third-parties.	Inspected the third-party and vendor policies and procedures to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the third-party and vendor policies and procedures to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the third-party and vendor policies and procedures to determine that the entity documented procedures for terminating third-party relationships.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement outlines and communicates confidentiality commitments and requirements.	Inspected the third-party master agreement and third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements.	No exceptions noted.
		Management assesses the compliance of confidential commitments and requirements of third-parties at least annually.	Inspected the evaluation forms to determine that management assessed the compliance of confidential commitments and requirements of third-parties at least annually.	No exceptions noted.
		The entity's third-party agreement outlines and communicates privacy commitments and requirements.	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated privacy commitments and requirements.	No exceptions noted.
		Management assesses the compliance of privacy commitments and requirements of third-parties at least annually.	Inspected the vendor risk register to determine that management assessed the compliance of privacy commitments and requirements of third-parties annually.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert generated from the monitoring software to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the annual future processing capacity demand forecast to determine that future processing demand was forecasted and compared to scheduled capacity on an annual basis.	No exceptions noted.
		Future processing demand forecasts are reviewed and approved by management on an annual basis.	Inspected the meeting minutes to determine that future processing demand forecasts were reviewed and approved by management on an annual basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	System data is encrypted during the replication process between cloud environments.	Inspected the backup replication configurations to determine that system data was replicated and encrypted via the cloud in real-time.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Senior Manager, Analytics Engineering 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 listing of users with the ability to recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated offsite by a third-party vendor in real time.	Inspected the contract with the offsite backup storage vendor to determine that backup media was replicated offsite by a third-party vendor in real time.	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups of certain application and database components are performed on a monthly basis and incremental backups are performed on a daily basis.	Inspected the backup schedule and configurations and a backup log for a sample of days to determine that full backups of certain application and database components were performed on a monthly basis and incremental backups were performed on a daily basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Production data is backed up and replicated to an offsite facility in real-time.	Inspected the backup replication configurations to determine that production data was backed up and replicated to an offsite facility real-time.	No exceptions noted.
		Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the business continuity and disaster recovery plans and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A data backup restoration test is performed on a weekly basis.	Inquired of the Senior Security Analyst regarding restoration testing to determine that a data backup restoration test was performed on a weekly basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed backup restoration test for a sample of weeks to determine that a data backup restoration test was performed on a weekly basis.	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.
		A business continuity and disaster recovery plan is 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.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagram and information security policy 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.
		For each critical system, the entity defines and documents what data and information is critical to support the system.	Inspected the system asset inventory, Information Classification Standard, and Information Security Program Standard to determine that for each critical system, the entity defined and documented what data and information was critical to support the system.	No exceptions noted.
		The entity has defined the following components of the data critical to supporting the system: • A description of what the critical data is and is used for • Source of the data • How the data is stored and transmitted	Inspected the system asset inventory, Information Classification Standard, and Information Security Program Standard to determine that the entity defined the following components of the data critical to supporting the system: • Description of what the critical data is and is used for • Source of the data • How the data is stored and transmitted	No exceptions noted.
		Management reviews the inventory of data and information that is critical to support the system for completeness and accuracy.	Inspected the database activity log to determine that management reviewed the inventory of data and information that was critical to support the system for completeness and accuracy.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity’s objectives.	Data is classified and structured in a consistent manner.	Inspected the system asset inventory, the database structure and the Information Classification Standard to determine that data was classified and structured in a consistent manner.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired the Senior Software Engineer regarding edit checks to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Observed the input of information into the in-scope system to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		The types of data input into the system by the entity's employees are defined and documented.	Inspected the system asset inventory, Information Classification Standard, and Information Security Program Standard to determine that the types of data inputted into the system by the entity's employees was defined and documented.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	The types of information input into the system by user entities is defined and documented.	Inspected the system asset inventory, Information Classification Standard, and Information Security Program Standard to determine that the types of information input into the system by user entities was defined and documented.	No exceptions noted.
		Processing power and CPU utilization performance requirements necessary for business operations are defined and documented.	Inspected the customer contract template and Information Security Program Standard to determine that processing power and CPU utilization performance requirements necessary for business operations were defined and documented.	No exceptions noted.
		Monitoring software is used to monitor processing power and CPU utilization.	Inspected the tool used to monitor processing power and CPU utilization to determine that monitoring software was used to monitor processing power and CPU utilization.	No exceptions noted.
		The entity has defined what critical data is processed and how it is processed.	Inspected the system asset inventory, Information Classification Standard, and Information Security Program Standard to determine that the entity defined what data was processed and how it was processed.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Errors in the processing of critical data are detected and corrected in a timely manner.	Inspected the system used to monitor the processing of critical data and the data processing error alert and supporting incident ticket for a sample of data processing errors to determine that errors in the processing of critical data were detected and corrected in a timely manner.	No exceptions noted.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	Critical data output from the system is stored and transmitted using secure encryption methods.	Inspected the encryption configurations for critical data outputted from the system that was stored and the encryption configurations for critical data outputted from the system that was transmitted to determine that critical data output from the system was stored and transmitted using secure encryption methods.	No exceptions noted.
		Access to critical data that is output from the system is restricted authorized parties.	Inquired of the Director of Information Security Operations regarding access to critical data to determine that access to critical data that was output from the system was restricted authorized parties.	No exceptions noted.
			Inspected the list of authorized parties that have access to critical data outputted from the system to determine that access to critical data to determine that access to critical data that was output from the system was restricted authorized parties.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	Procedures are in place to provide for the completeness, accuracy, and timeliness of critical data that is output from the system.	Inspected the system asset inventory, Information Classification Standard, and Information Security Program Standard to determine that procedures were in place to provide for the completeness, accuracy, and timeliness of critical data that was output from the system.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Critical data records are securely archived.	Inspected the encryption configurations for data at rest to determine that critical data records were securely archived.	No exceptions noted.
		Backups of critical data are maintained securely offsite by a third-party.	Inspected the contract with the offsite backup storage vendor and attestation report of the backup storage vendor to determine that backups of critical data were maintained offsite by a third-party.	No exceptions noted.
		Procedures are in place to provide for complete, accurate, and timely storage of data.	Inspected the Information Backups Policy and Information Security Program Standard to determine that procedures were in place to provide for complete, accurate, and timely storage of data.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ways in which critical data are backed up and stored are documented and reviewed annually.	Inspected the Information Backups Policy and Information Security Program Standard to determine that the ways in which critical data were backed up and stored were documented and reviewed annually.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Documented confidential policies and procedures are in place that include the following: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed	Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place that included: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed	No exceptions noted.
		An inventory is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the asset inventory to determine that an inventory was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.
		Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Principal Security Risk and Compliance Analyst regarding access to confidential information to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.2	The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.		Inspected the file access permissions for a file marked as confidential to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
		Confidential information is protected from erasure or destruction during the specified retention period.	Inspected the confidentiality policies and procedures to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the Record Retention Standard and destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
		An inventory is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the asset inventory to determine that an inventory was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented data destruction policies and procedures are in place that include the following: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	Inspected the data destruction policies and procedures to determine that documented data destruction policies and procedures were in place that included: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy				
P1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	The entity provides notice to the data subjects it collects personal information about including the following: • Purpose for collecting personal information • Choice and consent • Types of personal information collected • Methods of collection • Use, retention, and disposal of personal information • Access to personal information • Disclosure of personal information to third-parties • Security for privacy • Quality of personal information • Monitoring and enforcement If personal information is collected from sources other than the individual	Inspected the privacy policy and website notice to determine that the entity provided notice to the data subjects it collected personal information about including the following: • Purpose for collecting personal information • Choice and consent • Types of personal information collected • Methods of collection • Use, retention, and disposal of personal information • Access to personal information • Disclosure of personal information to third-parties • Security for privacy • Quality of personal information • Monitoring and enforcement If personal information is collected from sources other than the individual	No exceptions noted.
		The entity provides notice to data subjects before the time personal information is collected.	Inquired of the Senior Director, Compliance regarding personal information to determine that entity provided notice to data subjects before the time personal information was collected.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy				
P1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Observed the data subject registration process to determine that the entity provided notice to data subjects before the time personal information was collected.	No exceptions noted.
		The entity provides notice to data subjects before or as soon as changes to the Privacy Notice are made.	Inspected the company website to determine that the entity provided notice to data subjects before the entity changes its privacy notice or as soon as the privacy notice was changed.	No exceptions noted.
		The entity provides notice to data subjects before personal information is used for new purposes not previously identified.	Inspected the company website to determine that the entity provided notice to data subjects before personal information was used for new purposes not previously identified.	No exceptions noted.
		A description of the entity's activities performed as it relates to the collection of a data subject's personal information is included in the entity's Privacy Notice.	Inspected the privacy policy and website notice to determine that a description of the entity's activities performed as it relates to the collection of a data subject's personal information was included in the entity's privacy notice.	No exceptions noted.
		The entity's Privacy Notice is made available through the company's website and uses clear language.	Inquired of the Senior Director, Compliance regarding the privacy notice to determine that the entity's privacy notice was made available through the company's website and used clear language.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy				
P1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Observed the company's website and inspected the Privacy Notice to determine that the entity's Privacy Notice was made available through the company's website and used clear language.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Choice and Consent				
P2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	The Privacy Notice informs data subjects about the choices available to them with respect to the collection, use, and disclosure of personal information.	Inspected the privacy policy and website notice to determine that the privacy notice informed data subjects about the choices available to them with respect to the collection, use, and disclosure of personal information.	No exceptions noted.
		The Privacy Notice informs data subjects that consent is required to collect, use, and disclose personal information.	Inquired of the Senior Director, Compliance regarding data subject personal information to determine that the Privacy Notice informed data subjects that consent was required to collect, use, and disclose personal information.	No exceptions noted.
			Observed the data subject registration process to determine that the Privacy Notice informed data subjects that consent was required to collect, use, and disclose personal information.	No exceptions noted.
			Inspected the privacy policy and website notice to determine that the privacy notice informed data subjects that consent was required to collect, use, and disclose personal information.	No exceptions noted.
		The Privacy Notice informs data subjects of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.	Inspected the privacy policy and website notice to determine that the privacy notice informed data subjects of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Choice and Consent				
P2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Consent is obtained from data subjects prior to their personal information being collected.	Inquired of the Senior Director, Compliance regarding data subject consent to determine that consent was obtained from data subjects prior to their personal information being collected.	No exceptions noted.
			Observed the data subject registration process to determine that consent was obtained from data subjects prior to their personal information being collected.	No exceptions noted.
			Inspected the consent acknowledgement for a sample of data subjects to determine that consent was obtained from data subjects prior to their personal information being collected.	No exceptions noted.
		When information that was previously collected is used for purposes not previously identified in the Privacy Notice, the new purpose is added to the Privacy Notice, the data subject is notified, and consent is obtained prior to such new use or purpose.	Inspected the privacy consent form for a sample of data subjects to determine that when information that was previously collected was used for purposes not previously identified in the privacy notice, the new purpose was added to the privacy notice, the data subject was notified, and consent was obtained prior to such new use or purpose.	No exceptions noted.
		Explicit consent is obtained from the data subject when sensitive personal information is collected, used, or disclosed.	Inquired of the Senior Director, Compliance regarding data subject consent to determine that explicit consent was obtained from the data subject when sensitive personal information was collected, used, or disclosed.	No exceptions noted.

<table>
<tr><th colspan="5">ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY</th></tr>
<tr><th colspan="5">Privacy Criteria Related to Choice and Consent</th></tr>
<tr><th>P2.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Observed the data subject registration process to determine that explicit consent was obtained from the data subject when sensitive personal information was collected, used, or disclosed.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the consent acknowledgement for a sample of data subjects to determine that explicit consent was obtained from the data subject when sensitive personal information was collected, used, or disclosed.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Consent is obtained before personal information is transferred to or from a separate entity.</td><td>Inspected the privacy policy and the consent acknowledgement for a data subject to determine that consent was obtained before personal information was transferred to or from a separate entity.</td><td>No exceptions noted.</td></tr>
</table>

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Collection				
P3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	The collection of personal information is limited to what is defined in the Privacy Notice.	Inspected the privacy policy and website notice to determine that the collection of personal information was limited to what was defined in the privacy notice.	No exceptions noted.
		The methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained fairly, without intimidation or deception, and lawfully.	Inspected the privacy law matrix to determine that the methods of collecting personal information were reviewed by management before they were implemented to confirm that personal information was obtained fairly, without intimidation or deception, and lawfully.	No exceptions noted.
		Third-parties that collect personal information are reliable sources that collect information fairly and lawfully.	Inspected the website and privacy notice for the third-parties that collect personnel information to determine that third-parties that collected personal information were reliable sources that collected information fairly and lawfully.	No exceptions noted.
		Data subjects are informed if the entity develops or acquires additional information about them for its use.	Inspected the privacy policy and website notice to determine that data subjects were informed if the entity developed or acquired additional information about them for its use.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Collection				
P3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity’s objectives related to privacy.	Explicit consent is obtained from the data subject when sensitive personal information is collected, used, or disclosed.	Inquired of the Senior Director, Compliance regarding data subject consent to determine that explicit consent was obtained from the data subject when sensitive personal information was collected, used, or disclosed.	No exceptions noted.
			Observed the data subject registration process to determine that explicit consent was obtained from the data subject when sensitive personal information was collected, used, or disclosed.	No exceptions noted.
			Inspected the consent acknowledgement for a sample of data subjects to determine that explicit consent was obtained from the data subject when sensitive personal information was collected, used, or disclosed.	No exceptions noted.
		Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with the entity's Privacy Notice.	Inspected the privacy policy, website notice, and the consent acknowledgement for a sample of data subjects to determine that documentation of explicit consent for the collection, use, or disclosure of sensitive personal information was retained in accordance with the entity's Privacy Notice.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Use, Retention and Disposal				
P4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	Personal information is used only for the intended purposes for which it was collected and only when consent has been obtained.	Inspected the Privacy Notice and the consent acknowledgement and personal information collected for a data subject to determine that personal information was used only for the intended purposes for which it was collected and only when consent was obtained.	No exceptions noted.
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	Personal information is retained for no longer than required to fulfill the stated purposes as defined in the Privacy Notice.	Inspected the Privacy Notice and record retention schedule to determine that personal information was retained for no longer than required to fulfill the stated purposes as defined in the entity's privacy notice.	No exceptions noted.
		Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.	Inspected the Privacy Policy and Record Retention Standard to determine that policies and procedures were implemented to protect personal information from erasure or destruction during the specified retention period of the information.	No exceptions noted.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	Requests for deletion of personal information are documented and tracked.	Inquired of the Senior Director, Compliance regarding requests for deletion of personal information to determine that requests for deletion of personal information were documented and tracked.	No exceptions noted.
			Inspected the Privacy Policy to determine that requests for deletion of personal information were documented and tracked.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Use, Retention and Disposal				
P4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the deletion request ticket for a sample of requests for the deletion of personal information to determine that requests for deletion of personal information were documented and tracked.	Testing of the control activity disclosed that there were no requests for deletion of personal information during the review period.
		Personal information that is no longer retained is anonymized, disposed of, or destroyed.	Inquired of the Senior Director, Compliance regarding personal information that was no longer retained to determine that personal information that was no longer retained was anonymized, disposed of, or destroyed.	No exceptions noted.
			Inspected the Privacy Policy to determine that personal information that was no longer retained was anonymized, disposed of, or destroyed.	No exceptions noted.
			Inspected the deletion request ticket for a sample of requests for the deletion of personal information to determine that personal information that was no longer retained was anonymized, disposed of, or destroyed.	Testing of the control activity disclosed that there were no requests for deletion of personal information during the review period.
		Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.	Inspected the Record Retention Standard to determine that policies and procedures were implemented to erase or otherwise destroy personal information that was identified for destruction.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Access				
P5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	The identity of data subjects who request access to their personal information is authenticated before they are given access to their personal information.	Inspected the entity's privacy policy and website notice to determine that the identity of data subjects who requested access to their personal information was authenticated before they were given access to their personal information.	No exceptions noted.
		Data subjects are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	Inspected the privacy policy and website notice and the data access request repository to determine that data subjects were able to determine whether the entity maintained personal information about them and, upon request, obtained access to their personal information.	No exceptions noted.
		Personal information is provided to data subjects in an understandable and reasonable manner.	Inspected the personal information page to determine that personal information was provided to data subjects in an understandable and reasonable manner.	No exceptions noted.
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third-parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Data subjects are able to update or correct personal information held by the entity, and when their personal information is updated or corrected, the entity provides such updated or corrected information to any third-parties that were previously provided with the data subject's personal information.	Inspected the personal information page to determine that data subjects were able to update or correct personal information held by the entity, and when their personal information was updated or corrected, the entity provided such updated or corrected information to any third-parties that were previously provided with the data subject's personal information.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Disclosure and Notification				
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P6.1	The entity discloses personal information to third-parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	Privacy policies for handling personal information are communicated to third-parties to whom personal information is disclosed.	Inspected the third-party agreement template and contract for a sample of third-parties to whom personal information was disclosed to determine that privacy policies for handling personal information were communicated to third-parties to whom personal information was disclosed.	No exceptions noted.
		Personal information is disclosed to third-parties only for the purposes for which it was collected or created and only when consent has been obtained from the data subject.	Inspected the consent acknowledgement, the personal information collected about the data subject by a third-party and that third-party's contract for a data subject to determine that personal information was disclosed to third-parties only for the purposes for which it was collected or created and only when consent was obtained from the data subject.	No exceptions noted.
		Personal information is disclosed only to third-parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's Privacy Notice.	Inspected the website and privacy notice for the third-parties that collect personnel information to determine that personal information was disclosed only to third-parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Disclosure and Notification				
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Real-time monitoring is in place for critical vendors through the use of a third-party risk monitoring solution.	Inspected the vendor risk dashboard and an example of an investigation for a risk score change to determine that real-time monitoring was in place for critical vendors through the use of a third-party risk monitoring solution.	No exceptions noted.
		Personal information is disclosed to third-parties for new purposes or uses only with the prior consent of data subjects.	Inspected the consent acknowledgement and the personal information collected about the data subject by a third-party for a data subject to determine that personal information was disclosed to third-parties for new purposes or uses only with the prior consent of data subjects.	No exceptions noted.
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	The entity creates and maintains a record of authorized disclosures of personal information that is reviewed annually for completeness, accuracy, and timeliness.	Inspected the personal information repository to determine that the entity creates and maintained a record of authorized disclosures of personal information that was reviewed annually for completeness, accuracy, and timeliness.	No exceptions noted.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is reviewed annually for completeness, accuracy, and timeliness.	Inspected the customer service support dashboard and tracking tool to determine that the entity created and maintained a record of detected or reported unauthorized disclosures of personal information that was reviewed annually for completeness, accuracy, and timeliness.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Disclosure and Notification				
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P6.4	The entity obtains privacy commitments from vendors and other third-parties who have access to personal information to meet the entity’s objectives related to privacy. The entity assesses those parties’ compliance on a periodic and as-needed basis and takes corrective action, if necessary.	Personal information is disclosed only to third-parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's Privacy Notice.	Inspected the website and privacy notice for the third-parties that collect personnel information to determine that personal information was disclosed only to third-parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice.	No exceptions noted.
		The entity has procedures in place to evaluate that third-parties have effective controls in place to meet the terms of the agreement.	Inspected the Privacy Policy to determine that the entity had procedures in place to evaluate that third-parties had effective controls in place to meet the terms of the agreement.	No exceptions noted.
P6.5	The entity obtains commitments from vendors and other third-parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity’s objectives related to privacy.	A process exists for obtaining commitments from third-parties to report to the entity actual or suspected unauthorized disclosures of personal information.	Inspected the contract for a sample of third-parties to whom personal information was disclosed to determine that a process existed for obtaining commitments from third-parties to report to the entity actual or suspected unauthorized disclosures of personal information.	No exceptions noted.
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.	The entity has a process for providing notice of breaches and incidents to affected data subjects.	Inspected the privacy policy and website notice to determine that the entity had a process for providing notice of breaches and incidents to affected data subjects.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Disclosure and Notification				
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects’ personal information, upon the data subjects’ request, to meet the entity’s objectives related to privacy.	The types of personal information and related processes, systems, and third-parties involved in the handling of such information are identified.	Inspected the personal information repository to determine that the types of personal information and related processes, systems, and third-parties involved in the handling of such information were identified.	No exceptions noted.
		Requests to identify what personal information is held and disclosures of the data subjects' personal information are tracked, and information related to the requests is identified and communicated to data subjects.	Inspected the privacy policy and website notice and the personal information repository to determine that requests to identify what personal information was held and disclosures of the data subjects' personal information were tracked, and information related to the requests was identified and communicated to data subjects.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Quality				
P7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Personal information is reviewed annually for accuracy and completeness against the purposes for which it is intended to be used.	Inspected the quality assurance tool review dashboard to determine that personal information was reviewed annually for accuracy and completeness against the purposes for which it was intended to be used.	No exceptions noted.
		Personal information is reviewed annually for relevance against the purposes for which it is to be used.	Inspected the quality assurance tool review dashboard to determine that personal information was reviewed annually for relevance against the purposes for which it was to be used.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PRIVACY CATEGORY				
Privacy Criteria Related to Monitoring and Enforcement				
P8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	A process is in place to address inquiries, complaints, and disputes.	Inspected the Privacy Policy and website notice and the incident management policies and procedures to determine that a process was in place to address inquiries, complaints, and disputes.	No exceptions noted.
		Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes.	Inspected the privacy policy and website notice to determine that data subjects were informed about how to contact the entity with inquiries, complaints, and disputes.	No exceptions noted.
		Each complaint is addressed, and the resolution is documented and communicated to the individual.	Inspected the complaint tracking spreadsheet for a sample of complaints from data subjects to determine that each complaint was addressed, and the resolution was documented and communicated to the individual.	No exceptions noted.
		Instances of non-compliance against the Privacy Notice are documented and reported, and corrective and disciplinary measures are taken as appropriate.	Inspected the privacy policy and website notice to determine that instances of non-compliance against the privacy notice were documented and reported, and corrective and disciplinary measures were taken as appropriate.	No exceptions noted.
		The effectiveness of controls over personal information are reviewed annually.	Inspected the Cybersecurity Townhall slide deck and the entity's completed attestation report to determine that the effectiveness of controls over personal information were reviewed annually.	No exceptions noted.

SECTION 5

OTHER INFORMATION
PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1 CC1.5 CC2.2	Upon hire, personnel are required to acknowledge the code of conduct.	Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge code of conduct.	Testing of the control activity disclosed that the code of conduct was not acknowledged for 3 of 25 new hires sampled.	In the Workday Spring 2025R1 update (delivered from Workday March 15, 2025, and implemented by Prog in early May), Workday introduced more robust Learning tools, notably the Audience Builder feature. Per Workday release notes, 2025R1 delivers new Learning capabilities allowing precise audience criteria and campaign delivery configurations. We have since migrated away from the problematic campaign tool and now use Audience Builder to define dynamic groups (e.g. "Hire Date ≤ today and status = New Hire") tied directly to compliance training assignments. This ensures assignments are triggered automatically and with improved visibility into audience definitions. Outcome & Future Prevention • Immediate remediation: Audience Builder launched and verified for course auto-assignment • Audit compliance restored: New hires now consistently receive mandatory compliance training • Governance: Established review of audience definitions and assignment logs every 30-45 days

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management’s Response
CC4.1 CC7.1	Internal and external vulnerability scans are performed monthly and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results for a sample of months and the supporting ticket for a sample of critical vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	Testing of the control activity disclosed that remedial actions were not taken timely for 25 of 25 critical vulnerabilities identified.	We didn't have dedicated vulnerability management focused team till mid this year, we had huge backlog of vulnerabilities that teams are working to clear. 30-day SLA won’t be met till we are clear out of full backlog. Our cloud journey is helping mitigate legacy systems which will help eliminate many vulnerabilities. All AWS vulnerabilities were in our legacy AWS environment, and they were added new to the patching process and hence it took longer to remediate them.
CC4.2	Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the various assessments performed on the environment were documented, investigated and addressed.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely.	We didn't have dedicated vulnerability management focused team till mid this year, we had huge backlog of vulnerabilities that teams are working to clear. 30-day SLA won’t be met till we are clear out of full backlog. Our cloud journey is helping mitigate legacy systems which will help eliminate many vulnerabilities. All AWS vulnerabilities were in our legacy AWS environment, and they were added new to the patching process and hence it took longer to remediate them.
		Inspected the various assessments performed on the environment and supporting incident tickets for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that deviations identified from the various assessments performed on the environment were documented, investigated and addressed.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely.	

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management’s Response
	Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions.	Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely.	We didn't have dedicated vulnerability management focused team till mid this year, we had huge backlog of vulnerabilities that teams are working to clear. 30-day SLA won’t be met till we are clear out of full backlog. Our cloud journey is helping mitigate legacy systems which will help eliminate many vulnerabilities. All AWS vulnerabilities were in our legacy AWS environment, and they were added new to the patching process and hence it took longer to remediate them.
		Inspected the various assessments performed on the environment and supporting incident tickets for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that deviations identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that 25 from a sample of 25 vulnerabilities were not remediated timely.	