A-LIGN

PlanSource Benefits Administration, Inc.

Type 2 SOC 2

2023

PLANSOURCE

REPORT ON PLANSOURCE BENEFITS ADMINISTRATION, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, AND CONFIDENTIALITY

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

July 1, 2022 to June 30, 2023

Table of Contents

SECTION 1

ASSERTION OF PLANSOURCE BENEFITS ADMINISTRATION, INC. MANAGEMENT

ASSERTION OF PLANSOURCE BENEFITS ADMINISTRATION, INC. MANAGEMENT

July 15, 2023

We have prepared the accompanying description of PlanSource Benefits Administration, Inc.'s ('PlanSource' or 'the Company') Human Capital Management (HCM) and BenAdmin Services Systems titled "PlanSource Benefits Administration, Inc.'s Description of Its HCM and BenAdmin Services Systems throughout the period July 1, 2022 to June 30, 2023" (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 HCM and BenAdmin Services Systems that may be useful when assessing the risks arising from interactions with PlanSource's system, particularly information about system controls that PlanSource 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, and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

PlanSource uses Amazon Web Services, Inc. (AWS) to provide cloud hosting and managed security services, DataSite to provide colocation services, SecureWorks, Inc. (SecureWorks) to provide managed security services and Ultimate Software Group, Inc. (Ultimate Software) to provide HCM platform application development and hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PlanSource, to achieve PlanSource's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents PlanSource's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of PlanSource'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 PlanSource, to achieve PlanSource's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents PlanSource's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of PlanSource's controls.

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

a. the description presents PlanSource's HCM and BenAdmin Services Systems System that was designed and implemented throughout the period July 1, 2022 to June 30, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that PlanSource'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 organizations and user entities applied the complementary controls assumed in the design of PlanSource's controls throughout that period.
c. except for the matter described in the following paragraphs, the controls stated in the description operated effectively throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that PlanSource'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 PlanSource's controls operated effectively throughout that period.

The accompanying description states that controls are in place to restrict administrative network, operating system, database, and application access to authorized personnel. However, testing of the control activities associated with logical access to the network, operating system, database, and application layers disclosed that user access was not appropriately removed upon termination and thus users with administrative access retained inappropriate access to PlanSource's HCM and BenAdmin Services Systems. Consequently, we were unable to determine whether PlanSource's controls were operating effectively during the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the following Trust Services Criteria:

- 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".
- 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."
- 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".

Justin Kazmark
Vice President of Vendor Management
PlanSource Benefits Administration, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: PlanSource Benefits Administration, Inc.

Scope

We have examined PlanSource's accompanying description of its HCM and BenAdmin Services Systems titled "PlanSource Benefits Administration, Inc.'s Description of Its HCM and BenAdmin Services Systems throughout the period July 1, 2022 to June 30, 2023" (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, 2022 to June 30, 2023, to provide reasonable assurance that PlanSource's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, Processing Integrity, and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

PlanSource uses AWS to provide cloud hosting and managed security services, DataSite to provide colocation services, SecureWorks to provide managed security services and Ultimate Software to provide HCM platform application development and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PlanSource, to achieve PlanSource's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents PlanSource's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of PlanSource'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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PlanSource, to achieve PlanSource's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents PlanSource's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of PlanSource'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 PlanSource management to provide additional information and is not a part of the description. Information about PlanSource'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 PlanSource's service commitments and system requirements based on the applicable Trust Services Criteria.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

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

Description of Tests of Controls

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

Basis for Qualified Opinion

PlanSource states in its description that controls are in place to restrict administrative network, operating system, database, and application access to authorized personnel. However, testing of the control activities associated with logical access to the network, operating system, database, and application layers disclosed that user access was not appropriately removed upon termination and thus users with administrative access retained inappropriate access to PlanSource's HCM and BenAdmin Services Systems. Consequently, we were unable to determine whether PlanSource's controls were operating effectively during the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the following Trust Services Criteria:

- 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".
- 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."
- 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".

Opinion

In our opinion, except for the matter described in the preceding paragraphs, in all material respects,

a. the description presents PlanSource's HCM and BenAdmin Services Systems that was designed and implemented throughout the period July 1, 2022 to June 30, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that PlanSource'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 organizations and user entities applied the complementary controls assumed in the design of PlanSource's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that PlanSource'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 PlanSource's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4*,* is intended solely for the information and use of PlanSource, user entities of PlanSource's HCM and BenAdmin Services Systems during some or all of the period July 1, 2022 to June 30, 2023, business partners of PlanSource subject to risks arising from interactions with the HCM and BenAdmin Services Systems, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
July 15, 2023

SECTION 3

PLANSOURCE BENEFITS ADMINISTRATION, INC.'S DESCRIPTION OF ITS HCM AND BENADMIN SERVICES SYSTEMS THROUGHOUT THE PERIOD JULY 1, 2022 TO JUNE 30, 2023

OVERVIEW OF OPERATIONS

Company Background

PlanSource was founded in early 2007 and offers benefits and Human Resources (HR) professionals a means to select, implement and manage employee benefit programs for growing and medium-sized businesses. The company offers a platform capable of delivering self-service functionality in the areas of insurance procurement, customer onboarding, online enrollment, consolidated billing, and ongoing administration. The technology is designed to enable employers, brokers and insurance carriers to offer, enroll and manage a complete portfolio of employee benefits, healthcare products, and services.

Description of Services Provided

PlanSource BenAdmin

The PlanSource BenAdmin System provides employers with an online technology platform for benefits enrollment and year-round benefits management. It provides brokers with access to a broker portal where they can receive quotes from PlanSource's portfolio partners, configure administrator and employee sites for benefit content management and online enrollment, and perform day-to-day BenAdmin and management functions including premium billing. Brokers are the primary clients of PlanSource who then distribute the products throughout their client base.

There are three different models for delivering PlanSource BenAdmin Services:

Licensed BenAdmin

The broker provides the system to clients as a BenAdmin tool and performs the setup and support. The employer or broker performs day-to-day administration. The broker is also responsible for programming data feeds to carriers.

Co-Sourced BenAdmin

The broker provides the system to clients as a BenAdmin tool and performs the setup and support with PlanSource handling the data feeds and premium billing. The employer or broker performs day-to-day administration.

Outsourced BenAdmin

The broker provides the system to clients as a BenAdmin tool; however, PlanSource performs the setup, support, data feed management, and premium billing. The employer or broker performs day-to-day administration.

Human Capital Management (HCM)

The HCM platform helps customers to develop and implement HR and benefits strategies based on real-time business analytics and best practices. The employee and manager can access the information they need through the integrated portal. This product, delivered as HCM, combines payroll, benefit, and Human Resource Management (HRMS) technologies. To administer the benefits programs, PlanSource utilizes the proprietary, web-based BenAdmin technology integrated with the payroll and HRMS software. This solution allows customers to pass payroll and benefits data back and forth in real-time.

Principal Service Commitments and System Requirements

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

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

- Security principles within the fundamental designs of the HCM and BenAdmin Services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

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

Components of the System

Infrastructure

The HCM and BenAdmin Services Systems is limited to the services and infrastructure maintained by PlanSource at the Orlando, Florida; Charleston, South Carolina; Salt Lake City, Utah, USA and Bangalore India locations. The physical production systems are located at the DataSite Orlando third-party data center. DataSite is responsible for providing physical and environmental security that includes a secured data center facility with environmental control systems. The physical backup and disaster recovery systems are located at the AWS third-party data center. AWS is responsible for the physical and environmental security of those systems.

PlanSource's production systems are supported on physical and virtual machines. Multiple, redundant firewalls are implemented on the network perimeter to filter incoming traffic. In addition, an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are in place to analyze network traffic, block suspected network security breaches and detect inappropriate, incorrect or anomalous activity. The IPS and IDS are managed and monitored by SecureWorks. SecureWorks is responsible for monitoring of PlanSource's network IPS and IDS, analyzing network events, and reporting possible or actual network security breaches to PlanSource's information security personnel. Potential or actual network security breach incidents are reported by SecureWorks via e-mail and/or phone (depending on the severity of the security incident) and are reviewed by PlanSource's information security personnel.

Primary infrastructure used to provide PlanSource's HCM and BenAdmin Services Systems includes the following:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
PlanSource Benefits Application	Web-based, in-house developed application that manages benefits transactions, and educates employees through a self-service website that can be accessed by employers, employees, insurance carriers, and brokers	CentOS (64-bit) and Ubuntu (64-bit) including Percona / My Structured Query Language (SQL)	DataSite
UltiPro (HCM) Application	A third-party application that is utilized to support the HCM services and is developed and maintained by Ultimate Software	Windows .NET implementation	Not applicable - maintained by Ultimate Software
Benefits Application Backup Servers	Servers that provide backup and recovery	CentOS (64 bit) and Ubuntu (64-bit)	AWS
Virtual Hypervisor	Provides authentication and restricts access to virtual hosts	VMWare vCenter	DataSite
Storage Area Network (SAN) Storage	Stores the backup data	Dell EMC	DataSite
Firewall	Firewalls used to filter and route traffic	Cisco ASA	DataSite
Domain Controller	Active Directory restricts access to production systems to authorized and authenticated personnel	Microsoft Windows (64-bit)	DataSite

Software

Primary software used to provide PlanSource's HCM and BenAdmin Services Systems includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
UltiPro	(Hosted by Ultimate Software)	Primary application for HCM
BenAdmin	Ubuntu Linux	Primary application for PlanSource BenAdmin

People

- Executive Management - Responsible for establishment of product vision, overseeing of company-wide activities, and attainment of business objectives.
- Operations Management and Staff - Responsible for client implementation, renewal, account management, and day-to-day customer support. Additionally, monitors and manages inbound and outbound data flows and related processes.
- Information Technology (IT) Department - Manages, monitors, and supports information systems and responsible for day-to-day maintenance of system integrity, security, and availability.
- Software Development - Provides support for internally escalated issues from operations and IT departments.

Data

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
PlanSource BenAdmin Client data that may include the following (depending upon the scope of services provided): • Employee and Dependent demographic and enrollment data • Payroll data, such as, salary, salary history, organizational structure, job classifications and assignments, payroll schedules, paid time off data, W4 data, etc. • Personal health information (PHI) may be collected under certain service arrangements • Benefits and payroll business rules	Provides the following data (depending upon the scope of services provided) in various exports and reports: • Enrollment and participation reports • Dependent and beneficiary data • Eligibility exports • Carrier billing reports • Payroll deductions • Payroll and W-2 data	Confidential
HCM Client data that may include the following (depending upon the scope of services provided): • Payroll data, such as, pay history, direct deposit organizational structure, job classifications and assignments, payroll schedules, paid time off data, W2 data, etc. • Payroll tax filing data	Provides the following data (depending upon the scope of services provided) in various exports and reports: • Payroll processing and exception reports • New hire reports • Payroll tax reports	Confidential

Processes, Policies and Procedures

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

Physical Security

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

Logical Access

Access Authentication and Authorization

In order to access applications, data used in benefits processing, and financial reporting data, PlanSource users authenticate through the network layer. The network layer consists of access that is granted through PlanSource's Microsoft AD services. As part of this component, access to PlanSource desktops or servers requires a user account and password in Active Directory. Authentication rules are enforced through Active Directory including password minimum length, expiration, history, and account lockout requirements. Operating systems also utilize the network domain password settings as a component of the group policy settings that are applied locally. Linux operating system users and database users are required to authenticate via a user account, password, and unique encrypted Secure Shell (SSH) public key before being granted access to the operating system. Network domain administrator and server administrator privileges are restricted to user accounts accessible by authorized personnel.

For client access provisioning, PlanSource sets up an administrator account, which grants the designated individual(s) within the external organization access to provision modify, remove additional user accounts for their own organization. Client access is outside the boundaries of the system. Therefore, clients (user entities) are responsible for configuring the appropriate authentication parameters and providing appropriate access to authorized users.

Access Requests and Access Revocation

Access to PlanSource's systems is restricted by the implementation of identification, authentication, and authorization mechanisms. Prior to gaining access to the production systems, employees review and sign the code of conduct, confidentiality and non-disclosure agreement. In addition, new employees are required to complete security awareness training as a component of the hiring process and current employees are required to complete security awareness training on an annual basis. A new user request is submitted by HR personnel, within the issue tracking system, once the required components of the hiring process are completed. New user access requests include the date of the required request, location of the user, purpose of the request, etc. Once authorization is received, network/system administrators create the account based on the information within the access request.

When a user is terminated an access revocation request is submitted by HR personnel, within the issue tracking system. Access revocation requests include the date of the required request, location of the user, purpose of the request. Once received, the network/system administrators remove access based on the information within the revocation request.

Computer Operations - Backups

Automated backup systems are utilized to backup production servers. Full backups are performed on a weekly basis and incremental backups are performed on a daily basis to the disaster recovery site in Salt Lake City, Utah. An e-mail notification is sent to information security personnel and third-party system administrators regarding the success or failure of system backups. Upon receiving the notification, information security personnel and/or third-party system administrators determine the reason for the backup failure and make the necessary corrective action and determine if the backup needs to be run manually.

PlanSource has implemented a disaster recovery plan, which is updated on at least an annual basis by information security personnel. The disaster recovery plan includes the use of a third-party disaster recovery facility, which is provided by AWS. The plan is tested on at least an annual basis, and PlanSource management implements any required training or adjustments to the plan as a result of the testing. AWS is responsible for implementing and maintaining physical and environmental security controls around backup and disaster recovery infrastructure. PlanSource is responsible for monitoring the equipment and related services contained in the AWS data centers.

Computer Operations - Availability

PlanSource's infrastructure is configured for redundancy and is monitored for possible security violations. An enterprise monitoring application is utilized to monitor certain network devices to allow for centralized monitoring, including load utilization and network/database performance, and/or vulnerabilities. The enterprise monitoring application is configured to send e-mail notifications to information security personnel when predefined thresholds are exceeded on monitored network devices. Additionally, PlanSource has documented incident response procedures to define actions to be taken in the event of a security incident (e.g., virus infections, hacker attempts, improper disclosure of confidential information, system service interruptions, breach of personal information and other events with serious information security implications). An issue tracking log is utilized to document and monitor production incidents from identification to response and resolution.

A third-party vendor conducts quarterly scans of relevant external facing subnets which help to determine if vulnerability patching is needed to remediate a potential vulnerability to PlanSource systems. The quarterly scans display a risk factor which assists PlanSource in prioritizing vulnerability patching and overall remediation. Vulnerability assessments and application penetration testing is only completed for the Benefits application. HCM application vulnerability and application penetration testing is the responsibility of Ultimate Software. An enterprise level IPS and IDS is in place to monitor for suspicious activity and patterns of activity. SecureWorks is utilized to monitor the IPS and IDS, analyze network events, and report possible or actual network security breaches to information security personnel.

A patch management policy is documented to guide personnel through the patch management process. On a monthly basis, Microsoft patches are documented within the internal infrastructure ticketing system and require approval from the development operations team prior to implementation. A ticketing system is utilized to document the approval and implementation of patches. Linux patches are applied automatically to Linux servers on a weekly basis via a scheduled cron script.

Change Control

Changes to the benefits applications follow a standardized change management methodology. Changes are grouped to normal, urgent, or immediate priorities, and are scheduled for deployment in a release. Changes are required to be authorized by internal personnel. Changes, once authorized, are tracked in an internal ticketing system which contains information that includes, but not limited to, the following:

- Type of Change
- Change Requestor
- Change Details
- Test Cases, if applicable
- Change Approval

Infrastructure changes are categorized by routine, major, or emergency changes and tracked within an internal ticketing system which contains information that includes, but not limited to, the following:

- Type of Change
- Change Requestor
- Change Details
- Assigned Approver

GIT version control software is utilized to manage application development and maintenance activities and is configured to provide code check-in and check-out, version audit trails, restoration and rollback. Access privileges to promote changes into the PlanSource production environment are restricted to authorized users. Additionally, in order to help ensure that unauthorized changes are not made to the production environment, the following controls have been implemented:

- A cron script is utilized to alert IT management in the event of unauthorized changes made to production.
- A monthly review of checked-in code is performed by IT management.

Data Communications

PlanSource does not manage client data contained within any of the applications and databases hosted for clients. The completeness and accuracy of stored data is the customer's responsibility. PlanSource performs processing for BenAdmin clients that includes, but may not be limited to, processing for payroll and W2, and export translation of data to specified formats for carrier processing and enrollment at the carrier level. Please see the Trust Services Criteria Not Applicable to the In-Scope System section below for more details.

Boundaries of the System

The scope of this report includes the HCM and BenAdmin Services Systems performed in the Orlando, Florida; Charleston, South Carolina; Salt Lake City, Utah, USA and Bangalore, India locations facility.

This report does not include the cloud hosting and managed security services provided by AWS, the colocation services provided by DataSite Orlando, the managed security services provided by SecureWorks and the HCM platform application development and hosting services provided by Ultimate Software.

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

Control Environment

Integrity and Ethical Values

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

They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that PlanSource has implemented in this area are described below:

- The employee policy and procedures manual contain organizational policy statements and codes of conduct to which employees are required to adhere.

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

Board of Directors and Audit Committee Oversight

PlanSource's control consciousness is influenced significantly by the entity's board of directors and audit committee. Attributes include the board of directors' or audit committee's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with external auditors. Specific control activities that PlanSource has implemented in this area are described below:

- A board of directors oversees management activities.
- An audit committee oversees the independent third-party financial audit.

Commitment to Competence

PlanSource's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. PlanSource's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that PlanSource 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.
- Employees are required to sign the written position requirement indicating that they understand the requirements and expectations for the position they have accepted.

Management's Philosophy and Operating Style

PlanSource's management philosophy and operating style encompasses 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. Management meetings are held on a periodic basis to address issues as they are brought to management's attention. Specific control activities that PlanSource has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting services provided during the monthly management meeting.
- Management and employee meetings are held on an annual basis to discuss operational issues.

Organizational Structure and Assignment of Authority and Responsibility

PlanSource's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. PlanSource's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. PlanSource has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. PlanSource's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at helping to ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

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

HR Policies and Practices

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

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

- New employee hiring procedures are in place to guide the hiring process and pre-hire and new hire checklists are completed for new hires.
- Employees receive a 90-day evaluation from the date of hire and an annual evaluation.
- Employee termination procedures are in place to guide the termination process and termination checklists are completed for terminated employees.

Risk Assessment Process

PlanSource has placed a risk assessment process in operation to identify and manage risks that could affect the organization's ability to provide reliable HCM platform and outsourced BenAdmin services for user entities. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks.

Risk Identification

PlanSource has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Key members of the internal staff and executive management have identified and documented risks to the system. The process included identification of the business assets and associated business owners, which is followed by establishing threats, vulnerabilities, and risk levels.

Risk Factors

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

<u>External Factors</u>

- Technological developments.

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

Internal Factors

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

Risk Analysis

Risk analysis is an essential process to the entity's success. Each defined threat and vulnerability has been analyzed for controls that mitigate the risk. Risks that are not currently mitigated by controls are analyzed and projects are scheduled to implement controls that mitigate the associated risk. The control activities that are associated with the security, availability, processing integrity and confidentiality principles have been documented in the Testing Matrices.

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, processing integrity, and confidentiality principles.

Information and Communications Systems

Internal Communications

PlanSource has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for employees, and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate with their supervisor/manager or executive management.

If incidents are communicated, personnel follow documented incident response plan. For example, if a change in procedure is required, the project manager is advised of the change. Formal procedure changes are distributed to management before they are incorporated into the policy and distributed to relevant parties. Incidents are documented within the ticketing system and tracked by management until resolved.

External Communications

PlanSource has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include the use of e-mail messages and communication via the assigned account manager for time-sensitive information.

Monitoring Controls

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Senior management immediately evaluates the facts and circumstances related to any suspected control breakdowns. A decision for addressing any controls weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

On-Going Monitoring

Examples of PlanSource's ongoing monitoring activities include the following:

- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Regular review of incidents that are reported and documented by the information security team.
- Alert notifications received from automated backup systems and enterprise monitoring software.
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, penetration test reports, or automated patching systems.

Separate Evaluations

Examples of PlanSource's separate evaluations include the following:

- PlanSource management holds monthly operational meetings, including each department. Overall department performance, including customer feedback and current issues are reviewed, and impacts of new technology or laws and regulations that may impact services provided are also discussed.
- Monthly IT staff meetings are held to discuss current events, issues, emerging technologies and applicable laws or regulations that impact system security.

Subservice Organization Monitoring

PlanSource reviews the DataSite physical and environmental controls annually. Additionally, PlanSource reviews the results of network scans and vulnerability assessments as part of a quarterly report provided by Tenable.io. The application development and hosting services provided by Ultimate Software are monitored as part of normal business options, and IT management obtains and reviews the Ultimate Software third-party audit reports. The following monitoring activities are in place related to the services provided by AWS, DataSite, SecureWorks, and Ultimate Software:

- PlanSource reviews the results of the annual SOC examinations for AWS, DataSite, SecureWorks, and Ultimate Software.
- Results of network scans and vulnerability assessments performed by Tenable.io are reviewed on a quarterly basis.
- The application development and hosting services provided by Ultimate Software are monitored as part of normal business operations.
- SLAs are monitored for compliance as a part of normal business operations.

Reporting Deficiencies

The nature, timing and extent of the incidents identified are documented within an internal SharePoint, for management tracking and review. Deviations or deficiencies associated with controls are immediately escalated to management for immediate correction action. Results of third-party assessments and audits are reviewed by senior management, and corrective action, if required, is assigned to an individual and documented once those required actions are complete.

Changes to the System Since the Last Review

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

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 and Confidentiality criteria were applicable to the PlanSource HCM and BenAdmin Services Systems.

Subservice Organizations

The scope of this report includes the HCM and BenAdmin Services Systems performed in the Orlando, Florida; Charleston, South Carolina; Salt Lake City, Utah, USA and Bangalore, India locations facility.

This report does not include the cloud hosting and managed security services provided by AWS, the colocation services provided by DataSite Orlando, the managed security services provided by SecureWorks and the HCM platform application development and hosting services provided by Ultimate Software.

Subservice Description of Services

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

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

SecureWorks provides managed security services which includes monitoring controls and IDS and IPS management. SecureWorks' IDS and IPS management service provides 24/7 proactive administration, monitoring and maintenance of customer's IDS and IPS infrastructure.

Ultimate Software provides platform hosting services used to host the HCM application. This includes business continuity, physical security, logical security and change management controls for the housed in-scope systems. Controls include but are not limited to monitoring and logging of physical access to the facilities, business continuity and vulnerability management.

Complementary Subservice Organization Controls

PlanSource'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 all of the Trust Services Criteria related to PlanSource's services to be solely achieved by PlanSource control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of PlanSource.

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

Subservice Organization - AWS		
Category	**Reference**	**Control**
	CC6.4	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.

Subservice Organization - AWS		
Category	**Reference**	**Control**
Common Criteria/Security and Availability	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.
		Closed Circuit Television Cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is 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.
	A1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
		AWS maintains a formal risk management program to identify, analyze, treat and continuously monitor and report risks that affect AWS' business objectives and regulatory requirements. The program identifies risks, documents them in a risk register as appropriate, and reports results to leadership at least semi-annually.
		AWS has a process in place to review environmental and geo-political risks before launching a new region.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		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 and third-party colocation sites where Amazon maintains the UPS units.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.

Subservice Organization - AWS		
Category	**Reference**	**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.
		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.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
		AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.

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

Subservice Organization - DataSite Orlando		
Category	**Reference**	**Control**
Common Criteria/Security and Availability	CC6.4 CC7.2	Customer computer equipment is secured by locked cages or locked cabinets and the provided premises is exclusively occupied by only that specific customer.
		Access to each customer's computer equipment premises within the data center is restricted to appropriately authorized individuals.
		All DataSite Orlando employees, customers, vendors, and other visitors are recorded in the Master Record of Entry by the security officer or CET on duty.
		DataSite Orlando facility and data center is monitored by security officers 24 hours a day, 7 days a week, and 365 days a year.
		Surveillance cameras record access to the facility and data center and are viewable at all times by security officers.
		Video surveillance footage is recorded to a DVR (Digital Video Recorder) system and retained for one year.
		Customer access must be authorized by an appropriate approved customer designee or DataSite Orlando representative.
		Customers are issued a key to their exclusive computer equipment premises within the data center. The key is stored within the security officer station and is only issued upon verification of the person as they enter the facility.
		Access to the master key to the facility is limited to appropriate individuals.

Subservice Organization - DataSite Orlando		
Category	**Reference**	**Control**
		For deliveries, a DataSite Orlando representative meets the delivery party at the loading dock and freight is inspected.
		Upon exit, all customers are required to return to the security officer station to return their access badge and issued key.
		Access to digital media is restricted physically via locked cabinet and systematically within the Avigilon system.
		Access administration to the Avigilon system is restricted to appropriately authorized individuals.
	A1.2	Policies and procedures are documented to guide DataSite Orlando personnel activities for managing, operating and monitoring environmental equipment in the data center and facility.
		Maintenance contracts are in place to provide for appropriate maintenance of environmental safeguards.
		Facility personnel perform daily maintenance and inspection procedures over environmental equipment.
		Facility personnel maintain a central database to track regular preventative maintenance activities and unscheduled maintenance over all environmental equipment.
		The data center within the facility has raised floors with water, smoke and heat detection devices.
		The facility is equipped with fire detection and suppression systems which include: dry pipe sprinkler system, CO2 fire suppression, fire alarms, fire/smoke detectors, and handheld fire extinguishers.
		The facility is equipped with cooling plant with a redundant chiller system.
		The HVAC mechanical systems are inspected and preventative maintenance is performed on a regular basis.
		The facility is equipped with an UPS to provide the data center with a temporary power supply in the event of a power disruption.
		The UPS and critical power distributions systems are inspected on an annual basis.
		The facility is equipped with multiple engine powered generators that are redundant as a secondary power supply in the event of a power failure.
		The turbine powered generators and diesel powered generators are scheduled for preventative maintenance and inspection on a monthly and annual basis.
		The facility is equipped with an enterprise monitoring system to monitor certain environmental conditions.

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

Subservice Organization - SecureWorks		
Category	**Criteria**	**Control**
Common Criteria/Security and Availability	CC4.1 CC6.1 CC6.6 CC6.7 CC7.1 CC7.2 A1.1	Security monitoring applications are in place to analyze system activity and are configured to alert IT personnel when certain predefined thresholds have been reached.
		Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization and alert the information security team upon detection of unusual system activity or service request.

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

Subservice Organization - Ultimate Software		
Category	**Criteria**	**Control**
Common Criteria/Security, Processing Integrity and Availability	CC4.1 CC7.1	Penetration testing is performed on an annual basis. UKG evaluates vulnerabilities and tracks the vulnerabilities through the remediation process.
		UKG conducts periodic vulnerability scans of the environment and had developed a process for the review and resolution of vulnerabilities.
	CC5.1 CC7.5 A1.3	Business continuity planning (BCP) procedures are established and tested at least annually. The results of the BCP tests are reviewed by management.
	CC6.1 CC6.7 PI1.5	The storage on which customer data resides is encrypted.
	CC6.4 CC7.2	New physical access requests are formally documented and approved prior to access being granted.
		Physical Access is revoked timely in case of termination.
	CC6.6 CC6.8 CC7.2	Unless exempted by UKG management, antivirus software is installed and in continuous use in the production environment.
	CC8.1	Changes to the environment are documented in a change request, in accordance with UKG's policy.
		Changes to the environment are testing prior to implementation or validation in production, in accordance with UKG's policy.
		Changes to the environment are reviewed and approved, in accordance with UKG's policy.
		Access to migrate changes to production is restricted to authorized personnel.

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

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

PlanSource's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to PlanSource's services to be solely achieved by PlanSource control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of PlanSource'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 PlanSource.
2. User entities are responsible for notifying PlanSource of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of PlanSource 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 PlanSource services.
6. User entities are responsible for providing PlanSource with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying PlanSource of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for the completeness and accuracy of data entered into the system, data processed within the system and data output from the system.
9. User entities are responsible for reviewing the inventory of data and information that is critical to support the system for completeness and accuracy.
10. User entities are responsible for reviewing data input into the system for completeness, accuracy and timeliness.
11. User entities are responsible for configuring the appropriate authentication parameters and providing appropriate access to authorized users within the user entity's organization.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria/Security (to the Security, Availability, Processing Integrity and Confidentiality 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.

Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of PlanSource's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at PlanSource are described within Section 4 and within the "Subservice Organizations" section 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 PlanSource was limited to the Trust Services Criteria, related criteria and control activities specified by the management of PlanSource and did not encompass all aspects of PlanSource'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 employee handbook.	Inspected the employee handbook, the information security policies and procedures, the guide to general employment and employee benefits and the entity's SharePoint site to determine that core values were communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook is documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook was documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the employee handbook and code of conduct acknowledgement certificate for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the background investigation policy and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.

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**
		Upon hire, personnel are required to sign a confidentiality agreement.	Inspected the signed confidentiality agreement for a sample of new hires to determine that upon hire, personnel were required to sign a confidentiality agreement.	No exceptions noted.
		Personnel are required to acknowledge the ethics and code of conduct on an annual basis.	Inspected the ethics and code of conduct course completion and acknowledgement certificate for a sample of current employees to determine that personnel were required to acknowledge the ethics 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 completed performance and conduct evaluation tracking tool 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 employee handbook and the performance improvement plan policy to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
		Employees are directed on how to report unethical behavior.	Inspected the employee handbook to determine that employees were directed on how to report unethical behavior.	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**
		Third parties and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the entity's website to determine that third parties and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management 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 roles and responsibilities are documented and reviewed as needed.	Inspected the job description for a sample of executive management members to determine that executive management roles and responsibilities were documented reviewed as needed.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the completed executive performance review meeting minutes for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart, the information security policies and procedures and the completed internal controls matrix to determine that executive management maintained independence from those that operated the key controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the ISO internal control audit review meeting minutes, the security risk assessment slide deck and the completed internal controls matrix to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the completed performance and conduct evaluation tracking tool for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix, the information security policies and procedures, the ISO internal control audit review meeting minutes and the security risk assessment management meeting slide deck to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		The entity's organizational chart is updated in real-time.	Inspected the organizational chart to determine that the entity's organizational chart was updated in real-time.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Executive management reviews job descriptions and makes updates, if necessary.	Inspected the job description for a sample of job roles to determine that executive management reviewed job descriptions and made updates, if necessary.	No exceptions noted.
		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, the information security policies and procedures and the job description for a sample of job roles to determine that executive management had established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities 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 vendor management policies and procedures and the ISO information security risk management policies and procedures 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.
			Inspected the completed 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.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the guide to general employment and employee benefits policies and procedures and the compliance training and education policy 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 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 interview scorecard 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.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the job description and resume 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 third-party evaluation report and tracking tool 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 and resume 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.
		Upon hire, personnel are required to complete a background check.	Inspected the background investigation policy and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.

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 created a training program for its employees.	Inspected the information security awareness training program to determine that executive management had created a training program for its employees.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inquired of the Senior Director of HR, regarding information security training upon hire to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
			Inspected the compliance training and education policy to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
			Inspected the information security awareness training completion tracking tool for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the employee handbook and code of conduct acknowledgement certificate for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the ethics and code of conduct on an annual basis.	Inspected the ethics and code of conduct course completion and acknowledgement certificate for a sample of current employees to determine that personnel were required to acknowledge the ethics and code of conduct on an annual basis.	No exceptions noted.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the guide to general employment and employee benefits policies and procedures and the compliance training and education policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation tracking tool for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions and makes updates, if necessary.	Inspected the job description for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions and made updates, if necessary.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee handbook and the performance improvement plan policy to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired of the Senior Director of Operations, regarding the 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.
			Inspected the edit check configurations to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		A data flow diagram is documented and maintained by management to identify the critical data points and flow of information.	Inspected the data flow diagram to determine that a data flow diagram was documented and maintained by management to identify the critical data points and flow of information.	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 IDS and the IPS configurations, the encryption methods and configurations for data at rest and in transit, and the Virtual Private Network (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 are assessed annually for relevance and use.	Inspected the data retention and disposal policy and the supporting critical data assessment ticket to determine that data and information critical to the system were 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.	Inquired of the Senior Manager of Information Security Governance, Risk and Compliance (GRC), regarding data retention to determine that data was only retained for as long as required to perform the required system functionality, service, or use.	No exceptions noted.
			Inspected the data retention policies and procedures to determine that data was only retained for as long as required to perform the required system functionality, service, or use.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity’s policies and procedures, code of conduct and employee handbook are made available to personnel through the entity’s SharePoint site.	Inspected the entity’s SharePoint site to determine that the entity’s policies and procedures, code of conduct and employee handbook were made available to personnel through the entity’s SharePoint site.	No exceptions noted.
		Upon hire, personnel are required to read and acknowledge the information security policies and procedures.	Inspected the signed information security policies and procedures acknowledgement for a sample of new hires to determine that upon hire, personnel were required to read and acknowledge the information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to complete information security awareness training.	Inquired of the Senior Director of HR, regarding information security training upon hire to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
			Inspected the compliance training and education policy to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
			Inspected the information security awareness training completion tracking tool 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 read and acknowledge the information security policies and procedures annually.	Inspected the information security training course completion and acknowledgement tracker for a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures annually.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the information security awareness training completion form for a sample of current employees to determine that management tracked and monitored compliance with information security and awareness training requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the employee handbook and code of conduct acknowledgement certificate for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the ethics and code of conduct on an annual basis.	Inspected the ethics and code of conduct course completion and acknowledgement certificate for a sample of current employees to determine that personnel were required to acknowledge the ethics and code of conduct on an annual basis.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the product and tech townhall slide deck and the annual operation planning meeting slide 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.
		Employees are directed on how to report unethical behavior.	Inspected the employee handbook to determine that employees were directed on how to report unethical behavior.	No exceptions noted.
		Third parties and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the entity’s website to determine that 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**
		Changes to job roles and responsibilities are communicated to personnel through the entity's SharePoint site.	Inspected the entity's SharePoint site to determine that changes to job roles and responsibilities were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		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 site.	Inspected the ISO cyber security incident management policy and procedures and the entity's SharePoint site 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 site.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreements delineate the boundaries of the system and describes relevant system components.	Inspected the master business process outsourcing services agreement to determine that the entity's third-party agreements delineated the boundaries of the system and described relevant system components.	No exceptions noted.
			Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreements delineated the boundaries of the system and described relevant system components.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreements communicate the system commitments and requirements of third parties.	Inspected the master business process outsourcing services agreement to determine that the entity's third-party agreements communicated the system commitments and requirements of third parties.	No exceptions noted.
			Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreements communicated the system commitments and requirements of third parties.	No exceptions noted.
		The entity's third-party agreements outline and communicate the terms, conditions and responsibilities of third parties.	Inspected the master business process outsourcing services agreement to determine that the entity's third-party agreements outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
			Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreements outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inquired of the Senior Manager of Information Security GRC, regarding customer agreements to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the master software as a service agreement, the master software as a service reseller agreement and the master end user agreement to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the executed agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	Testing of the control activity disclosed that a contract was not in place for 2 of the 25 customers sampled.
		The entity's contractor agreements outline and communicate the terms, conditions and responsibilities of external users.	Inspected the master contractor agreement to determine that the entity's contractor agreements outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via updated agreements.	Inquired of the Senior Manager of Information Security GRC, regarding changes to commitments, requirements and responsibilities to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users and customers via updated agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the updated agreement to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users and customers via updated agreements.	No exceptions noted.
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and shared with external parties.	Inquired of the Senior Manager of Information Security GRC, regarding escalation procedures for external parties to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and shared with external parties.	No exceptions noted.
			Inspected the master software as a service agreement, the master software as a service reseller agreement and the master end user agreement to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and shared with external 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**
		Executive management meets annually with operational management to discuss the results of assessments performed by third parties.	Inspected the ISO internal control audit review meeting minutes, the security risk assessment management meeting slide deck and the completed internal controls matrix to determine that executive management met annually with operational management to discuss the results of assessments performed by third parties.	No exceptions noted.
		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 business process outsourcing services 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.
			Inspected the executed third-party agreement for a sample of third parties 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to commitments and requirements relating to confidentiality are communicated to third parties, external users, and customers via updated agreements.	Inquired of the Senior Manager of Information Security GRC, regarding changes to commitments and requirements relating to confidentiality 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.
			Inspected the entity's 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, the employee performance evaluation policies and procedures, the information security program charter and the entity's annual operation planning slide deck to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's annual operation planning slide deck and the information security program charter 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 ISO information security risk management policies and procedures to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected the completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the revision history of the entity's policies and procedures to determine that executive management reviewed policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.
		Executive management reviews and addresses control failures.	Inspected the risk register, the ISO internal control audit review meeting minutes, the security risk assessment slide deck and the risk register review meeting minutes for a sample of months to determine that executive management reviewed and addressed control failures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of internal control failures to determine that executive management reviewed and addressed control failures.	No exceptions noted.
		Executive management has established key performance indicators for operational controls effectiveness, including the acceptable level of control operation and failure.	Inspected the key performance indicators for operational controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart, the information security policies and procedures and the completed internal controls matrix 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 key performance indicators for operational and internal controls effectiveness to determine that the entity had defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures, the entity's annual operation planning slide deck and the key performance indicators for business and employee performance 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 annual operation planning slide deck and the information security program charter to determine that business plans and budgets aligned with the entity's strategies and 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**
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the entity's annual operation planning slide deck and the information security program charter 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 the ISO framework.	Inspected the completed internal controls matrix and the information security policies and procedures to determine that the entity's internal controls framework was based on the ISO framework.	No exceptions noted.
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inquired of the Senior Manager of Information Security GRC, regarding the internal controls environment to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.
			Inspected the completed internal controls matrix, the policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	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**
		Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives.	Inspected the entity's annual operation planning slide deck, the information security program charter, the policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the ISO information security risk management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		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 ISO information security risk management policies and procedures to determine that management had 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 an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's risk assessment process includes: • Setting the context and scope of assessment • Identification and prioritization of the threats to Information Resources • Identification and prioritization of the vulnerabilities of Information Resources • Identification of a threat that may exploit a vulnerability • Qualitative and/or quantitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific gap • Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources	Inspected the ISO information security risk management policies and procedures to determine that the entity's risk assessment process included: • Setting the context and scope of assessment • Identification and prioritization of the threats to Information Resources • Identification and prioritization of the vulnerabilities of Information Resources • Identification of a threat that may exploit a vulnerability • Qualitative and/or quantitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific gap • Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that the entity's risk assessment process included: • Setting the context and scope of assessment • Identification and prioritization of the threats to Information Resources • Identification and prioritization of the vulnerabilities of Information Resources • Identification of a threat that may exploit a vulnerability • Qualitative and/or quantitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific gap • Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources	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 ISO information security risk management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		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 ISO information security risk management policies and procedures 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.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the ISO information security risk management policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the ISO information security risk management policies and procedures to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
			Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the ISO information security risk management policies and procedures to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
			Inspected the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.	Inspected the ISO information security risk management policies and procedures to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third parties.	No exceptions noted.
			Inspected the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third parties.	No exceptions noted.

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**
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud (loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	Inspected the completed risk assessment to determine that on an annual basis, management identified and assessed the types of fraud (loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	No exceptions noted.
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed risk assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the ISO information security risk management policies and procedures to determine that changes to the regulatory, economic and physical environment in which the entity operated were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the regulatory, economic and physical environment in which the entity operated 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 ISO information security risk management policies and procedures to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the ISO information security risk management policies and procedures to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the ISO information security risk management policies and procedures to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the ISO information security risk management policies and procedures to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software settings, the IDS and IPS configurations, and the firewall rulesets for a sample of production servers 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 revision history of the entity's policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the completed internal controls matrix and the completed internal audit results 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.
		Logical access reviews are performed annually.	Inquired of the Senior Manager of Information Security GRC, regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed user access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inquired of the Senior Manager of Information Security GRC, regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		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 to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans 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**
		A third-party performs a penetration test 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 test annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation tracking tool for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report and management's review for a sample of third parties to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		A formal risk assessment is performed on 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				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the ISO internal control audit review meeting minutes, the security risk assessment slide deck and the risk register review meeting minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and control failures/gaps identified as part of the compliance, control and risk assessments performed.	Inspected the ISO internal control audit review meeting minutes, the security risk assessment slide deck and the risk register review meeting minutes to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.

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 communicated to those parties responsible for taking corrective actions.	Inspected the risk assessment, the vulnerability scan results for a sample of months, the penetration test results and the internal audit results 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 supporting incident ticket for a sample of vulnerabilities identified from the vulnerability scans and penetration test 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 supporting incident ticket for a sample of control failures identified from the internal audit assessment 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**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inspected the risk assessment, the vulnerability scan results for a sample of months, the penetration test results and the internal audit results 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 supporting incident ticket for a sample of vulnerabilities identified from the vulnerability scans and penetration test 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 supporting incident ticket for a sample of control failures identified from the internal audit assessment 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.

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 addressed by those parties responsible for taking corrective actions.	Inspected the risk assessment, the vulnerability scan results for a sample of months, the penetration test results and the internal audit results 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 supporting incident ticket for a sample of vulnerabilities identified from the vulnerability scans and penetration test 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 supporting incident ticket for a sample of control failures identified from the internal audit assessment 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**
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the entity's risk register, the ISO internal control audit review meeting minutes, the security risk assessment slide deck and the risk register review meeting minutes 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.	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 and the completed internal controls matrix 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.	Inspected the risk register, the vulnerability scan results for a sample of months, the penetration test results and the ISO internal audit results 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 supporting incident ticket for a sample of vulnerabilities identified from the vulnerability scans and penetration test 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.

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 a sample of control failures identified from the internal audit assessment 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.
		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, the information security policies and procedures 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 documented the relevant controls in place for each key business or operational process.	Inspected the information security policies and procedures and the completed internal controls matrix to determine that management had 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 information security policies and procedures and the completed internal controls matrix to determine that management had incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the ISO information security risk management policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment and the completed internal controls matrix to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures 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**
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans, including revision history to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that the business continuity and disaster recovery plan were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and the completed internal controls matrix to determine that an analysis of incompatible operational duties was performed on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	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.

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**
CC5.2	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 site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the information security policies and procedures and the completed internal controls matrix to determine that management had 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 information security policies and procedures and the completed internal controls matrix to determine that management had established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	Inspected the information security policies and procedures and 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 information security policies and procedures and the completed internal controls matrix to determine that management had established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 had 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.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart, the information security policies and procedures 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.
		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.
		Process owners and management investigate and troubleshoot control failures.	Inspected the completed risk assessment and the completed internal controls matrix to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures to determine that process owners and management investigated and troubleshot control failures.	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**
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected the completed internal controls matrix, the ISO internal audit report, the ISO internal control audit review meeting minutes and the security risk assessment slide deck to determine that effectiveness of the internal controls implemented within the environment were evaluated annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the ISO asset management policy to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
			Inspected the asset inventory listing and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	Testing of the control activity disclosed that an asset inventory was not completely and accurately maintained. As such, A-LIGN could not confirm an asset inventory listing was maintained of assets with confidential data. Subsequent testing of the control activity through inspection of the risk register disclosed that remediation efforts were in place to remediate this gap prior to end of the review period.

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**
	Internal Network - Okta			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of IT Support and Engineering, 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 roles 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 Senior Director of IT Support and Engineering, regarding administrative access to the network to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access roles to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Password length • Complexity	Inspected the network password configurations to determine that the network was configured to enforce password requirements that included: • Password history • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Director of IT Support and Engineering, regarding network authentication to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the network to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that network users were authenticated via individually assigned user accounts and passwords.	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 configurations 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • 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 • Logon events • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Windows Active Directory			
		Production network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of IT Support and Engineering, regarding production network access to determine that production 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 production network user listing and access roles to determine that production network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production network administrative access is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding administrative access to the production network to determine that production network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production network administrator listing and access roles to determine that production network administrative access was restricted to authorized personnel.	No exceptions noted.
		Production network is configured to enforce password requirements that include: • Password history • Password length • Complexity	Inspected the production network password configurations to determine that production networks were configured to enforce password requirements that included: • Password history • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production network users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Director of IT Support and Engineering, regarding production network authentication to determine that production network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the production network to determine that production network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the production network user listing and password configurations to determine that production network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production network account lockout configurations to determine that production network 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 network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Servers - Windows, Linux			
		Production server user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of IT Support and Engineering, 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.

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 server user listing and access roles 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 Director of IT Support and Engineering, regarding administrative access to the production servers 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 server administrative access was restricted to authorized personnel.	No exceptions noted.
		Production server users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Director of IT Support and Engineering, regarding production server authentication to determine that production server users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the production servers to determine that production server 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**
			Inspected the production server user listings and password configurations to determine that production server users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production server account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the account lockout configurations for the 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 • Logon events • Object access • Policy changes • Privilege use • System events	Inspected the production server audit logging configurations 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 • Logon events • Object access • Policy changes • Privilege use • 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 server audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the production server audit logs to determine that production server audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production server audit log extract to determine that production server audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Databases - MySQL Server			
		Production databases user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of IT Support and Engineering, regarding production databases 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 database user listing and access roles 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**
		Production databases administrative access is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding administrative access to the production databases to determine that production databases administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production databases administrator listing and access roles to determine that production databases administrative access was restricted to authorized personnel.	No exceptions noted.
		Production databases are configured to enforce password requirements that include: • Password history • Password length • Complexity	Inspected the password configurations for the production database to determine that production databases were configured to enforce password requirements that included: • Password history • Password length • Complexity	No exceptions noted.
		Production databases users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Director of IT Support and Engineering, regarding production database authentication 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**
			Observed the authentication of a user to the production databases to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the production database user listings and password configurations to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production databases account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the account lockout configurations for the production databases to determine that production databases 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 databases audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the production database audit logs to determine that production databases audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that production databases audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Applications - BenAdmin and HCM			
		Production application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of Operations, 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.

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 administrative access is restricted to authorized personnel.	Inquired of the Senior Director of Operations, regarding administrative access to the production application to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production application administrator listing and access roles to determine that production application administrative access was restricted to authorized personnel.	Testing of the control activity disclosed that 11 of the 90 administrative users retained administrative access to the production application BenAdmin after termination. Subsequent testing of the control activity disclosed the VPN access was removed timely for the 11 users.
		The production applications are configured to enforce password requirements that include: • Password length • Complexity	Inspected the production applications password configurations to determine that production applications were configured to enforce password requirements that included: • Password length • Complexity	No exceptions noted.
		Production application users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Director of Operations, regarding production application authentication to determine that production application 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**
			Observed the authentication of a user to the production applications to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			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.
		Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production applications account lockout configurations to determine that production application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production applications audit logging configurations and an example 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.

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 logs are maintained and available for review when needed.	Inquired of the Senior Director of Operations, regarding the production application audit logs to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.
	Remote Access - AnyConnect VPN			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of IT Support and Engineering, 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 to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding administrative access to the VPN to determine that the ability to administer VPN 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 VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication username and password prior to being granted remote access to the system.	Inquired of the Senior Director of IT Support and Engineering, regarding VPN authentications to determine that VPN users were authenticated via multi-factor authentication, username and password prior to being granted remote access to the system.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that VPN users were authenticated via multi-factor authentication, username and password prior to being granted remote access to the system.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication, username and password prior to being granted remote access to the system.	No exceptions noted.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inquired of the Senior Manager of Information Security GRC, regarding the entity’s networks to determine that the entity's various networks were segmented to keep information and data isolated and 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 network diagram, the internal firewall configurations, the Demilitarized Zone (DMZ) configurations, the Network Address Translation (NAT) configuration and Virtual Local Area Network (VLAN) configurations 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 network diagram, the IDS and IPS configurations and the firewall rulesets for a sample of production servers 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 DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ configurations 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 Secure Socket Layer/Transport Layer Security (SSL/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 SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the Senior Manager of Information Security GRC, 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 policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the Senior Manager of Information Security GRC, regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed user access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager of Information Security GRC, regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access control policies and procedures, the in-scope user listings, and the supporting 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 from personnel as a component of the termination process.	Inquired of the Senior Manager of Information Security GRC, regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
			Inspected the access control policies and procedures to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
			Inspected in-scope user listings and the supporting 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.	Testing of the control activity disclosed that access was not revoked timely for 2 of the 13 terminated employees sampled. Subsequent testing of the control activity through inspection of the network user access listing disclosed that network access was removed for the 2 terminated employees.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager of Information Security GRC, regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the access control policies and procedures, the in-scope user listings, and the supporting 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 from personnel as a component of the termination process.	Inquired of the Senior Manager of Information Security GRC, regarding the termination process to determine that logical access to systems was revoked from personnel 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 access control policies and procedures to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
			Inspected in-scope user listings and the supporting 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.	Testing of the control activity disclosed that access was not revoked timely for 2 of the 13 terminated employees sampled. Subsequent testing of the control activity through inspection of the network user access listing disclosed that network access was removed for the 2 terminated employees.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding privileged access to add, remove, or modify access to determine that privileged access 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 networks, operating systems and databases to determine that privileged access 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 applications to determine that privileged access add, remove, or modify access to user accounts was restricted to authorized personnel.	Testing of the control activity disclosed that privileged access to add, remove, or modify access to user accounts within the production application BenAdmin was not appropriate for 11 of the 90 administrative users. Subsequent testing of the control activity disclosed the VPN access was removed timely for the 11 users.
		Logical access reviews are performed annually.	Inquired of the Senior Manager of Information Security GRC, regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed user access review for the in-scope systems to determine that logical access reviews were performed annually.	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	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	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**
	least privilege and segregation of duties, to meet the entity's objectives.	Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager of Information Security GRC, regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the access control policies and procedures, the in-scope user listings, and the supporting 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 from personnel as a component of the termination process.	Inquired of the Senior Manager of Information Security GRC, regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
			Inspected the access control policies and procedures to determine that logical access to systems was revoked from personnel 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 in-scope user listings and the supporting 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.	Testing of the control activity disclosed that access was not revoked timely for 2 of the 13 terminated employees sampled. Subsequent testing of the control activity through inspection of the network user access listing disclosed that network access was removed for the 2 terminated employees.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding privileged access to add, remove, or modify access to determine that privileged access 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 networks, operating systems and databases to determine that privileged access 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 applications to determine that privileged access add, remove, or modify access to user accounts was restricted to authorized personnel.	Testing of the control activity disclosed that privileged access to add, remove, or modify access to user accounts within the production application BenAdmin was not appropriate for 11 of the 90 administrative users. Subsequent testing of the control activity disclosed the VPN access was removed timely for the 11 users.
		Logical access reviews are performed annually.	Inquired of the Senior Manager of Information Security GRC, regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed user access review for the in-scope systems to determine that logical access reviews were performed annually.	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 organizations. Refer to the "Subservice Organizations" section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	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 backup servers, per a defined schedule.	Inquired of the Senior Manager of Information Security GRC, regarding purging of data of backup servers to determine that the entity purged data stored on backup servers, per a defined schedule.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures and the backup schedule and configurations to determine that the entity purged data stored on backup servers, per a defined schedule.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inquired of the Senior Manager of Information Security GRC, regarding the data disposal process to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures 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**
			Inspected the data disposal tracking tool to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, the VPN authentication configurations and the digital certificates to determine that VPN, SSL/TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication username and password prior to being granted remote access to the system.	Inquired of the Senior Director of IT Support and Engineering, regarding VPN authentications to determine that VPN users were authenticated via multi-factor authentication, username and password prior to being granted remote access to the system.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that VPN users were authenticated via multi-factor authentication, username and password prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication, username and password prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Director of IT Support and Engineering, 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 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**
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Senior Director of IT Support and Engineering, 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 Director of IT Support and 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 roles 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**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rulesets for a sample of 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 firewall rulesets for a sample of 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 an IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and an IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection.	Inspected the IDS and IPS notification configurations and an example alert to determine that the IDS and IPS were configured to notify personnel upon intrusion detection.	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**
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The centralized antivirus software provider pushes updates to the installed antivirus software on workstations as new updates/signatures are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed antivirus software on workstations as new updates/signatures were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		Antivirus software is installed on 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 configurations for a sample of servers to determine that antivirus software was installed on servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.

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 antivirus software configurations for a sample of servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		The antivirus software is configured to scan servers in real-time.	Inspected the antivirus software configurations for a sample of servers to determine that the antivirus software was configured to scan servers in real-time.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		Data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the asset management policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and 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 roles to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated to an offsite facility daily.	Inspected the backup replication configurations and an example backup replication log to determine that backup data was replicated to an offsite facility daily.	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 encrypted during the replication process between cloud environments.	No exceptions noted.
		The ability to restore backups is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding access to restore backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups 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**
		VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, the VPN authentication configurations and the digital certificates to determine that VPN, SSL/TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Senior Director of IT Support and Engineering, 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rulesets for a sample of 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 firewall rulesets for a sample of 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.
		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.
		An IDS and an IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and an IPS were 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**
		The IDS and IPS are configured to notify personnel upon intrusion detection.	Inspected the IDS and IPS notification configurations and an example alert to determine that the IDS and IPS were configured to notify personnel upon intrusion detection.	No exceptions noted.
		Data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Backup data is stored in an encrypted format.	Inspected the encryption configurations for backup data to determine that backup data was stored in an encrypted format.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the asset management policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the Senior Manager of Information Security GRC, regarding the applications and software installation to determine that the ability to install applications and software on workstations 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 workstation installation configurations related to applications and software on workstations to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Manager of the ITS Support Team, regarding the change implementation process to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the listing 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.
		A code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that a code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures and the ISO systems development lifecycle (SDLC) security policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The centralized antivirus software provider pushes updates to the installed antivirus software on workstations as new updates/signatures are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed antivirus software on workstations as new updates/signatures were available.	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 centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		Antivirus software is installed on 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 configurations for a sample of servers to determine that antivirus software was installed on servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configurations for a sample of servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		The antivirus software is configured to scan servers in real-time.	Inspected the antivirus software configurations for a sample of servers to determine that the antivirus software was configured to scan servers in real-time.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures.	Inspected the ISO infrastructure security policy to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security policies and procedures to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	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 settings, the IDS and IPS configurations, and the firewall rulesets for a sample of production servers 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 monitoring system alert and the IDS and IPS notification configurations and an example IDS and IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS and an IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and an IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection.	Inspected the IDS and IPS notification configurations and an example alert to determine that the IDS and IPS were configured to notify personnel upon intrusion detection.	No exceptions noted.
		A code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that a code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the asset management policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rulesets for a sample of 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 firewall rulesets for a sample of 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.
		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 to determine that internal and external vulnerability scans were performed monthly and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans 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**
		A third-party performs a penetration test 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 test annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the ISO cyber security incident response 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.
		Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security policies and procedures to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 settings, the IDS and IPS configurations, and the firewall rulesets for a sample of production servers 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 monitoring system alert and the IDS and IPS notification configurations and an example IDS and IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDS and an IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and an IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection.	Inspected the IDS and IPS notification configurations and an example alert to determine that the IDS and IPS were configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that a code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rulesets for a sample of 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 firewall rulesets for a sample of 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**
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The centralized antivirus software provider pushes updates to the installed antivirus software on workstations as new updates/signatures are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed antivirus software on workstations as new updates/signatures were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		Antivirus software is installed on 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 configurations for a sample of servers to determine that antivirus software was installed on servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configurations for a sample of servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		The antivirus software is configured to scan servers in real-time.	Inspected the antivirus software configurations for a sample of servers to determine that the antivirus software was configured to scan servers in real-time.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the asset management policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
	Internal Network - Okta			
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout configurations 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • 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 • Logon events • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Windows Active Directory			
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production network account lockout configurations to determine that production network 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				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available 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 Servers - Windows, Linux			
		Production server account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the account lockout configurations for the 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 • Logon events • Object access • Policy changes • Privilege use • System events	Inspected the production server audit logging configurations 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 • Logon events • Object access • Policy changes • Privilege use • System events	No exceptions noted.
		Production server audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the production server audit logs to determine that production server audit logs were maintained and available 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 an example production server audit log extract to determine that production server audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Databases - MS SQL Server			
		Production databases account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the account lockout configurations for the production databases to determine that production databases 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 databases audit logs are maintained and available for review when needed.	Inquired of the Senior Director of IT Support and Engineering, regarding the production database audit logs to determine that production databases audit logs were maintained and available 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 an example production database audit log extract to determine that production databases audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Application - BenAdmin and HCM			
		Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production applications account lockout configurations to determine that production application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production applications audit logging configurations and an example 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 and available for review when needed.	Inquired of the Senior Director of Operations, regarding the production application audit logs to determine that production application audit logs were maintained and available 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 an example production application audit log extract to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	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 ISO cyber security incident response 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 annually for effectiveness.	Inspected the revision history of the ISO cyber security incident management policy and procedures to determine that the incident response and escalation procedures were reviewed annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on severity.	Inspected the ISO cyber security incident management policy and procedures to determine that the incident response policies and procedures defined the classification of incidents based on 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**
		Incidents are documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	Inquired of the Senior Manager of Information Security GRC, regarding the incident management process to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the ISO cyber security incident management policy and procedures to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident document for a sample of incidents to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that incidents were not tracked completely and accurately within the incident tracking log.
		Resolution of incidents are documented and communicated to affected users.	Inspected the supporting incident document for a sample of incidents to determine that resolution of incidents were documented and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Manager of Information Security GRC, regarding critical incident management to determine that security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the ISO cyber security incident management policy and procedures to determine that security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no critical incidents occurred during the review period.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Senior Manager of Information Security GRC, regarding critical incident management to determine that incidents resulting in the unauthorized use or disclosure of personal information were 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 HIPAA breach notification policy to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	No exceptions noted.
			Inspected the supporting incident document for a sample of critical security incidents that resulted in an unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	Testing of the control activity disclosed that no critical incidents resulting in the unauthorized use or disclosure of personal information occurred during the review period.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the ISO cyber security incident management policy 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.
		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 ISO cyber security incident response 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**
		Incidents are documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	Inquired of the Senior Manager of Information Security GRC, regarding the incident management process to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the ISO cyber security incident management policy and procedures to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident document for a sample of incidents to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that incidents were not tracked completely and accurately within the incident tracking log.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inspected the supporting incident document 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.

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**
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through e-mails.	Inquired of the Senior Manager of Information Security GRC, regarding critical incident management to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through e-mails.	No exceptions noted.
			Inspected the ISO cyber security incident response policies and procedures to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through e-mails.	No exceptions noted.
			Inspected the supporting incident document and e-mails for a sample of critical security incidents that resulted in a service/business operation disruption to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through e-mails.	Testing of the control activity disclosed that no critical incidents resulting in a service/business operation disruption occurred during the review period.
		Resolution of incidents are documented and communicated to affected users.	Inspected the supporting incident document for a sample of incidents to determine that resolution of incidents were documented and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remediation actions taken for security incidents are documented and communicated to affected users.	Inspected the supporting incident document for a sample of incidents to determine that the remediation actions taken for security incidents were documented and communicated to affected users.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Manager of Information Security GRC, regarding critical incident management to determine that security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the ISO cyber security incident management policy and procedures to determine that security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no critical 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 risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting incident ticket for a sample of vulnerabilities identified from the vulnerability scans and penetration test to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management reviews reports on an annual 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 security risk assessment slide deck to determine that management reviewed reports on an annual 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security policies and procedures, the ISO cyber security incident management policy, the backup policies and procedures, the business continuity plan and the change management policies and procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • 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 data backup restoration test is performed on an annual basis.	Inquired of the Senior Manager of Information Security GRC, regarding restoration testing to determine that a data backup restoration test was performed 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**
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Management reviews reports on an annual 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 security risk assessment slide deck to determine that management reviewed reports on an annual 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 Senior Manager of Information Security GRC, regarding critical incident management to determine that security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the ISO cyber security incident management policy and procedures to determine that security incident analysis was performed for critical incidents 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 security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no critical incidents occurred during the review period.
		A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		The business continuity and disaster recovery plan are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that the business continuity and disaster recovery plan were tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans and the 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				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures and the ISO SDLC security policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests - Change Review Board • Development - Development Team • Testing - Developer and Business Unit Effected • Implementation - Software Change Management Group	Inquired of the Manager of the ITS Support Team, regarding change management roles and responsibilities to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Change Review Board • Development - Development Team • Testing - Developer and Business Unit Effected • Implementation - Software Change Management Group	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the change management policies and procedures and the ISO SDLC security policy to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Change Review Board • Development - Development Team • Testing - Developer and Business Unit Effected • Implementation - Software Change Management Group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the release notes for an example system release to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		The ability to migrate/merge changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Manager of the ITS Support Team, regarding the change implementation process to determine that the ability to migrate/merge changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listing of users with the ability to migrate/merge changes into the production environment to determine that the ability to migrate/merge changes into the production environment was restricted to authorized and appropriate 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.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the code repository to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		Development and test environments are logically separated from the production environment.	Inspected the separate development, test, and production environments to determine that development and test environments were logically separated from the production environment.	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**
		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.
		System changes are documented within a ticket and pull request (PR) and are tracked through the change process to implementation.	Inspected the supporting change ticket for a sample of infrastructure, database and application changes to determine that system changes were documented within a ticket and pull request (PR) and were tracked through the change process to implementation.	No exceptions noted.
		A code/peer 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/peer review was systematically required prior to deploying the PR into the production environment.	No exceptions noted.
		A code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that a code repository was utilized to help detect unauthorized changes within the production environment.	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**
		A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from code repository to determine that the code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Backout capabilities allow for rollback of application changes when changes impair system operation.	Inspected the rollback capabilities within the code repository to determine that backout capabilities allow for rollback of application changes when changes impaired system operation.	No exceptions noted.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change 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 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**
		System patches/security updates follow the standard change management process.	Inspected the ISO configuration management policy to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for the configuration of IT systems and tools.	Inspected the information security policies and procedures and the ISO configuration management policy to determine that information security policies and procedures documented the baseline requirements for the 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 hot patch deployment 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 using data masking software that replaces confidential 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 confidential information with test information during 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**
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the ISO information security risk management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the ISO information security risk management policies and procedures to determine that management had 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 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 ISO information security risk management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		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 ISO information security risk management policies and procedures 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.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the ISO information security risk management policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity had purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor management policies and procedures and the ISO information security risk management policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor management policies and procedures and the ISO information security risk management policies and procedures to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor management policies and procedures and the ISO information security risk management policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the completed 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**
		The entity's third-party agreements outline and communicate: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship • Confidentiality	Inspected the master business process outsourcing services agreement to determine that the entity's third-party agreements outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship • Confidentiality	No exceptions noted.
			Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreements outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship • Confidentiality	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report and management's review for a sample of third parties to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor management policies and procedures and the ISO information security risk management policies and procedures 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.
			Inspected the completed 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.

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 has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	Inspected the organizational chart and the Chief Information Security Officer job description to determine that management had assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third parties.	Inspected the vendor management policies and procedures to determine that the entity had documented procedures for addressing issues identified with third parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the vendor management policies and procedures to determine that the entity had documented procedures for terminating third-party relationships.	No exceptions noted.
		The entity's third-party agreements outline and communicate confidentiality commitments and requirements.	Inspected the master business process outsourcing services agreement to determine that the entity’s third-party agreements outlined and communicated confidentiality commitments and requirements.	No exceptions noted.
			Inspected the executed third-party agreement for a sample of third parties to determine that the entity’s third-party agreements outlined and communicated confidentiality commitments and requirements.	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 assesses the compliance of confidential commitments and requirements of third parties annually.	Inspected the vendor management review meeting minutes and the vendor tracking tool to determine that management assessed the compliance of confidential 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 settings, the IDS and IPS configurations, and the firewall rulesets for a sample of production servers 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 monitoring system alert and the IDS and IPS notification configurations and an example IDS and IPS alert notification 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.
		Future processing demand is forecasted and compared to scheduled capacity on an annual basis.	Inquired of the Senior Manager of Information Security GRC, regarding future processing demand forecasting to determine that future processing demand was forecasted and compared to scheduled capacity 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**
			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.	Inquired of the Senior Manager of Information Security GRC, regarding future processing demand forecasting to determine that future processing demand forecasts were reviewed and approved by management on an annual basis.	No exceptions noted.
			Inspected the future processing demand review meeting minutes to determine that future processing demand forecasts were reviewed and approved by management on an annual basis.	No exceptions noted.
		The change management process is followed when a change is made to a system as a result of capacity constraint.	Inspected the supporting change ticket for a sample of changes made to a system as a result of a capacity issue to determine that the change management process was followed when a change was made to a system as a result of capacity constraint.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.

ADDITIONAL CRITERIA FOR THE 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.	Full backups of certain application and database components are performed on a weekly basis and incremental backups are performed on a daily basis.	Inspected the backup schedule and configurations and the backup log for an example day and an example week to determine that full backups of certain application and database components were performed on a weekly basis and incremental backups were performed on a daily basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected the backup schedule and configurations and the backup alert for a sample of backup failures 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.
		The ability to restore backups is restricted to authorized personnel.	Inquired of the Senior Director of IT Support and Engineering, regarding access to restore backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
		Production data is backed up and replicated to an offsite facility daily.	Inspected the backup replication configurations to determine that production data was backed up and replicated to an offsite facility daily.	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**
		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 policy, procedures and plans, the network diagram and the backup replication configurations 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 organizations. Refer to the “Subservice Organizations” section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A business continuity plan and disaster recovery plan are documented and in place that outline the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery policy, procedures and plans to determine that a business continuity and disaster recovery plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The business continuity plan and disaster recovery plan are tested on an annual basis and includes: • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery plan test results to determine that the business continuity plan and disaster recovery plan were tested on an annual basis and included: • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inquired of the Senior Manager of Information Security GRC, regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.

ADDITIONAL CRITERIA FOR THE 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.	A data flow diagram is documented and maintained by management to identify the critical data points and flow of information.	Inspected the data flow diagram to determine that a data flow diagram was documented and maintained by management to identify the critical data points and flow of information.	No exceptions noted.
		For each critical system, the entity defines and documents what data and information are critical to support the system.	Inspected the database tables and data structure, the ISO asset management policy and the data classification policy 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 database tables and data structure, the ISO asset management policy, the data classification policy, the cryptographic and key management policy and the backup policy and procedures to determine that the entity defined the following components of the data critical to supporting the system: • A description of what the critical data was and was used for • Source of the data • How the data was stored and transmitted	No exceptions noted.
		Data is classified and structured in a consistent manner.	Inspected the database tables and data structure to determine that data was classified and structured in a consistent manner.	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.	The types of information input into the application by user entities is defined and documented.	Inspected the data classification policies and procedures, the privacy policy and the database tables and data structure to determine that the types of information input into the application by user entities was defined and documented.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired of the Senior Director of Operations, regarding the 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.
			Inspected the edit check configurations to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	Monitoring software is used to monitor processing power and Central Processing Unit (CPU) utilization.	Inspected the tools 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 and how it is processed.	Inspected the data classification policies and procedures, the privacy policy and the database tables and data structure 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 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.	A data flow diagram is documented and maintained by management to identify the critical data points and flow of information.	Inspected the data flow diagram to determine that a data flow diagram was documented and maintained by management to identify the critical data points and flow of information.	No exceptions noted.
		For each critical system, the entity defines and documents what data and information are critical to support the system.	Inspected the database tables and data structure, the ISO asset management policy and the data classification policy 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 types of information input into the application by user entities is defined and documented.	Inspected the data classification policies and procedures, the privacy policy and the database tables and data structure to determine that the types of information input into the application by user entities was defined and documented.	No exceptions noted.
		Critical data output from the system is stored and transmitted using secure encryption methods.	Inspected the encryption configurations for critical data at rest and in transit to determine that critical data output from the system was stored and transmitted using secure encryption methods.	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.	Data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that 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 and the critical backup replication configurations 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 data center vendor to determine that backups of critical data were maintained offsite by a third-party.	No exceptions noted.
			Inspected the attestation report of the offsite data center 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 backup policies and procedures to determine that procedures were in place to provide for complete, accurate, and timely storage of data.	No exceptions noted.
		The ways in which critical data is backed up and stored is documented and reviewed annually.	Inspected the backup policies and procedures to determine that the ways in which critical data was backed up and stored was documented and reviewed annually.	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**
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	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 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 was required to achieve the purpose for which the data was collected and processed	No exceptions noted.
		An asset inventory listing is maintained of assets with confidential data.	Inspected the ISO asset management policy to determine that an asset inventory listing was maintained of assets with confidential data.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the asset inventory listing to determine that an asset inventory listing was maintained of assets with confidential data.	Testing of the control activity disclosed that an asset inventory was not completely and accurately maintained. As such, A-LIGN could not confirm an asset inventory listing was maintained of assets with confidential data. Subsequent testing of the control activity through inspection of the risk register disclosed that remediation efforts were in place to remediate this gap prior to end of the review period.
		Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Senior Manager of Information Security GRC, regarding access to confidential information and appropriateness of the Database Administrators (DBAs) to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
			Inspected the file access permissions for an example file marked as confidential, the DBA user access listing and the organizational chart 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.

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.	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, the asset management policies and procedure and the data classification policy to determine that documented data destruction policies and procedures were in place that included the following: • Identifying confidential information requiring destruction when the end of the retention period was reached • Erasing or destroying confidential information that had been identified for destruction	No exceptions noted.
		An asset inventory listing is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the ISO asset management policy to determine that an asset inventory listing 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**
			Inspected the asset inventory listing to determine that an asset inventory listing was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	Testing of the control activity disclosed that an asset inventory was not completely and accurately maintained. As such, A-LIGN could not confirm an asset inventory listing was maintained of assets with confidential data. Subsequent testing of the control activity through inspection of the risk register disclosed that remediation efforts were in place to remediate this gap prior to end of the review period.
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Senior Manager of Information Security GRC, regarding the data disposal process for confidential data to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures and the ISO asset management policy to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the data disposal tracking tool to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	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
CC2.3	Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the executed agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	Testing of the control activity disclosed that a contract was not in place for 2 of the 25 customers sampled.	A project is underway to update all contracts for customers and is expected to complete by EOY.
CC6.1	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the asset inventory listing and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	Testing of the control activity disclosed that an asset inventory was not completely and accurately maintained. As such, A-LIGN could not confirm an asset inventory listing was maintained of assets with confidential data. Subsequent testing of the control activity through inspection of the risk register disclosed that remediation efforts were in place to remediate this gap prior to end of the review period.	A project is in progress to align all asset management tools to create a complete inventory and assign owners and asset details (OS, use, sensitive data present, etc.).
	Production application administrative access is restricted to authorized personnel.	Inspected the production application administrator listing and access roles to determine that production application administrative access was restricted to authorized personnel.	Testing of the control activity disclosed that 11 of the 90 administrative users retained administrative access to the production application BenAdmin after termination. Subsequent testing of the control activity disclosed the VPN access was removed timely for the 11 users.	An automated user access review process is currently being deployed to allow for more frequent access and access level reviews. PlanSource is currently evaluating end to end IAM products for management of access creation and removal.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC6.1, CC6.2, CC6.3,	Logical access to systems is revoked from personnel as a component of the termination process.	Inspected in-scope user listings and the supporting 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.	Testing of the control activity disclosed that access was not revoked timely for 2 of the 13 terminated employees sampled. Subsequent testing of the control activity through inspection of the network user access listing disclosed that network access was removed for the 2 terminated employees.	An automated user access review process is currently being deployed to allow for more frequent access and access level reviews. PlanSource is currently evaluating end to end IAM products for management of access creation and removal.
CC6.2, CC6.3	Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inspected the listing of privileged users to the in-scope applications to determine that privileged access add, remove, or modify access to user accounts was restricted to authorized personnel.	Testing of the control activity disclosed that privileged access to add, remove, or modify access to user accounts within the production application BenAdmin was not appropriate for 11 of the 90 administrative users. Subsequent testing of the control activity disclosed the VPN access was removed timely for the 11 users.	An automated user access review process is currently being deployed to allow for more frequent access and access level reviews. PlanSource is currently evaluating end to end IAM products for management of access creation and removal.
CC6.6, CC6.8, CC7.2	Antivirus software is installed on 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 configurations for a sample of servers to determine that antivirus software was installed on servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.	As a part of improving asset management processes, systems lacking antivirus are now identified through scanning and are being updated with all required security controls.
	The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software configurations for a sample of servers and an example antivirus update log to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.	As a part of improving asset management processes, systems lacking antivirus are now identified through scanning and are being updated with all required security controls.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
	The antivirus software is configured to scan servers in real-time.	Inspected the antivirus software configurations for a sample of servers to determine that the antivirus software was configured to scan servers in real-time.	Testing of the control activity disclosed that antivirus software was not installed on 19 of the 28 servers sampled.	As a part of improving asset management processes, systems lacking antivirus are now identified through scanning and are being updated with all required security controls.
CC7.3, CC7.4	Incidents are documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident document for a sample of incidents to determine that incidents were documented and tracked within SharePoint folders and an incident tracking log and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that incidents were not tracked completely and accurately within the incident tracking log.	Plansource is evaluating Jira as an incident tracking platform rather than continuing to use manual spreadsheets for the master log.
C1.1	An asset inventory listing is maintained of assets with confidential data.	Inspected the asset inventory listing to determine that an asset inventory listing was maintained of assets with confidential data.	Testing of the control activity disclosed that an asset inventory was not completely and accurately maintained. As such, A-LIGN could not confirm an asset inventory listing was maintained of assets with confidential data. Subsequent testing of the control activity through inspection of the risk register disclosed that remediation efforts were in place to remediate this gap prior to end of the review period.	A project is in progress to align all asset management tools to create a complete inventory and assign owners and asset details (OS, use, sensitive data present, etc.).

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
C1.2	An asset inventory listing 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 listing to determine that an asset inventory listing was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	Testing of the control activity disclosed that an asset inventory was not completely and accurately maintained. As such, A-LIGN could not confirm an asset inventory listing was maintained of assets with confidential data. Subsequent testing of the control activity through inspection of the risk register disclosed that remediation efforts were in place to remediate this gap prior to end of the review period.	A project is in progress to align all asset management tools to create a complete inventory and assign owners and asset details (OS, use, sensitive data present, etc.).