VectorVMS
Type 2 SOC 2
2020

REPORT ON VECTORVMS' 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

November 1, 2019 to October 31, 2020

Table of Contents

SECTION 1

ASSERTION OF VECTORVMS MANAGEMENT

ASSERTION OF VECTORVMS MANAGEMENT

February 19, 2021

We have prepared the accompanying description of VectorVMS' ('VectorVMS' or 'service organization') Vendor Management System titled "VectorVMS' Description of Its Vendor Management System throughout the period November 1, 2019 to October 31, 2020" (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 Vendor Management System that may be useful when assessing the risks arising from interactions with VectorVMS' system, particularly information about system controls that VectorVMS 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*).

VectorVMS uses Cyxtera, Inc. ('Cyxtera') to provide colocation services and Iron Mountain, Inc. ('Iron Mountain') to provide backup tape rotation and storage 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 VectorVMS, to achieve VectorVMS' service commitments and system requirements based on the applicable trust services criteria. The description presents VectorVMS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of VectorVMS' 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 VectorVMS, to achieve VectorVMS' service commitments and system requirements based on the applicable trust services criteria. The description presents VectorVMS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of VectorVMS' controls.

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

a. the description presents VectorVMS' Vendor Management System that was designed and implemented throughout the period November 1, 2019 to October 31, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that VectorVMS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of VectorVMS' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that VectorVMS' 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 VectorVMS' controls operated effectively throughout that period.

John Cole
Vice President, Hosting Systems and Operations
PeopleFluent on behalf of VectorVMS

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: VectorVMS

Scope

We have examined VectorVMS' accompanying description of its Vendor Management System titled "VectorVMS' Description of Its Vendor Management System throughout the period November 1, 2019 to October 31, 2020" (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 November 1, 2019 to October 31, 2020, to provide reasonable assurance that VectorVMS' 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*).

VectorVMS uses Cyxtera to provide colocation services and Iron Mountain to provide backup tape rotation and storage services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at VectorVMS, to achieve VectorVMS' service commitments and system requirements based on the applicable trust services criteria. The description presents VectorVMS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of VectorVMS' 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 VectorVMS, to achieve VectorVMS' service commitments and system requirements based on the applicable trust services criteria. The description presents VectorVMS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of VectorVMS' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

Inherent Limitations

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

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

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects:

a. the description presents VectorVMS' Vendor Management System that was designed and implemented throughout the period November 1, 2019 to October 31, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that VectorVMS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of VectorVMS' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that VectorVMS' 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 VectorVMS' 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 VectorVMS, user entities of VectorVMS' Vendor Management System during some or all of the period November 1, 2019 to October 31, 2020, business partners of VectorVMS subject to risks arising from interactions with the Vendor Management System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
February 19, 2021

SECTION 3

VECTORVMS’ DESCRIPTION OF ITS VENDOR MANAGEMENT SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2019 TO OCTOBER 31, 2020

OVERVIEW OF OPERATIONS

Company Background

Learning Technologies Group plc, formerly known as PeopleFluent, Inc., (“PeopleFluent”) acting by and through its division VectorVMS (“VectorVMS”) offers vendor management solutions (VMS) that enables organizations to find, engage, and manage contingent workforces. The VectorVMS platform automates the entire process of procuring and managing contingent labor, from requisition to invoice and payment - allowing organizations to control costs, maintain compliance, and drive quality and efficiency throughout the contingent labor life cycle. A part of Learning Technologies Group plc (LTG), VectorVMS also powers a total talent ecosystem that gives clients a holistic view of their contingent and full-time workforce.

Description of Services Provided

VectorVMS, a former division of PeopleFluent, delivers software and services to help businesses optimize their contingent workforce programs.

VectorVMS works closely with clients and partners - drawing on 20 years of experience to combine the right people, process, and technology to design and implement best-fit vendor management solutions. With their Vendor Management System (VMS), Human Resources (HR) and procurement teams can control costs, maintain compliance, and drive quality and efficiency throughout the contingent labor lifecycle.

VectorVMS delivery models are the most flexible in the industry. VectorVMS empowers clients to manage strategic sourcing entirely in-house or through one of many trusted managed service providers (MSPs). Using the Shared Managed Services (SMS) program, VectorVMS can augment client resources with a team of experienced program managers who provide operational support, white-glove service, and advice on industry best practices. A part of Learning Technologies Group Inc., VectorVMS also powers a total talent ecosystem that gives clients a holistic view of their contingent and full-time workforce.

Principal Service Commitments and System Requirements

VectorVMS designs its processes and procedures related to Vendor Management System to meet its objectives for its Vendor Management services. Those objectives are based on the service commitments that VectorVMS makes to user entities, the laws and regulations that govern the provision of Vendor Management services, and the financial, operational, and compliance requirements that VectorVMS has established for the services.

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 Vendor Management System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

VectorVMS establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in VectorVMS’ 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 Vendor Management System.

Components of the System

Infrastructure

Primary infrastructure used to provide VectorVMS' Vendor Management System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Computer Server	HP Proliant	Application and database server platforms
Networking Switch	Cisco	Networked device connectivity
Network Firewall	Checkpoint and Cisco	Network traffic filtering
Network NIDS	Cisco	Network intrusion monitoring and alerting
File Storage Appliance	NetApp	Data storage
Content Switch	F5 BigIP	Web application load balancing and security

Software

Primary software used to provide VectorVMS' Vendor Management System includes the following:

Primary Software	
Software	**Purpose**
VectorVMS VMS	VMS software
MS Server	Windows server operating system
MS SQL	Database System
Business Intelligence	Application reporting
Nagios	System monitoring

People

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

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- Quality assurance (QA) team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Security and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by PeopleFluent in delivering its Vendor Management System. Such data includes, but is not limited to, the following:

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

Processes, Policies and Procedures

VectorVMS has adopted a framework for defining and controlling security. The framework defines VectorVMS' approach to security at the physical, network, operating system, database and application system layers. The framework addresses physical security, user authentication, access control, encryption, isolation and auditing and is designed to help ensure that the security criteria for VectorVMS are in place.

Physical Security

Cyxtera, Inc ("Cyxtera") controls the US data centers that house the VMS production and disaster recovery infrastructure. Cyxtera also controls the UK data center which houses the VMS production infrastructure in the United Kingdom. VectorVMS submits an Access Request ticket to Cyxtera for visitors that will need access to a datacenter. Cyxtera requires badge and biometric hand scanner authentication for VectorVMS and Cyxtera employees to enter the datacenters and VectorVMS cages and or equipment cabinets. Cyxtera retains visitors' government IDs in exchange for security badges to help ensure that badges do not leave either data center facility.

Approved physical access to the Cyxtera datacenters by VectorVMS or PeopleFluent employees is administered by the PeopleFluent Information Security department. Management performs a review of data center access on an annual basis. Cage and cabinet door access logs from the access control system are reviewed monthly by the PeopleFluent Information Security department. The data centers in the US, UK, and Canada are logically accessible from the Raleigh location. Members of the Operations Department have access via private point-to-point circuit connectivity to the servers in their physical zone. Network access control restrictions are based on network and static Internet Protocol (IP) addresses to help ensure that unknown computers cannot connect in the Operations physical zone and gain access to the data center's servers.

Physical access to the Raleigh and Waltham facilities is restricted via badge access system. In addition, members of the Global Technology Operations department or members of the Corporate Information Technology (IT) Operations department escort individuals requiring access to the corporate data centers that do not have access via the card scanning system. PeopleFluent's Information Security department maintains a list of users with access to the corporate datacenters and performs a review on an annual basis.

Badge Access System

The facility is secured using a badge access system. The system prevents entry of any unauthorized access throughout the Raleigh facility. Authorized individuals are given access to various security zones in the building based on their job or visiting function requirements. An individual should scan his/her card to enter secured zones within the facility. Information Security department employees grant access to the specified zones within the facility. The Information Security department is notified via email from Human Resources when new employees are hired and granted access based on their job function. This email serves as written approval from HR that access should be granted.

The badge access system records and logs individuals' movements throughout the facility. As directed by the VectorVMS Physical Security Policy, employees are required to scan their cards individually when entering a room to help ensure coat-tailing does not occur and employees' activity is appropriately logged. Non-functional visitor tags, which do not allow access to any zones, are distributed daily to guests. Visitors should be escorted to and from different zones by VectorVMS personnel. Contractors are issued temporary badges that grant access to common area zones. This helps to ensure that visitors are not granted access to sensitive areas. Visitor tags and temporary badges are kept in a locked drawer at the receptionist's area. Visitor tags and temporary card numbers are recorded in a log with the time, date and name of the individual they are being issued to the following rooms which contain sensitive information, require a scanned card to gain access:

- Reception
- Wiring Closets
- General work areas
- Computer rooms

VectorVMS revokes terminated employees' physical access to the VectorVMS facility. Terminated employees' access is revoked within 24 hours, following notification from Human Resources. Communications are sent out to a predefined group of personnel for employee on-boarding and termination processing. VectorVMS has a terminated employee checklist that includes steps to remove network and physical access when an employee leaves the Company.

For specific controls implemented by Cyxtera and Iron Mountain, please refer to the 'Subservice Organizations' section below.

Logical Access

Authentication Controls

The Operating System environment (Windows Server) is configured to require a User-ID and password to gain access to the system. VectorVMS domain security policies enforce the following minimum authentication criteria for the Operating System:

- Each user should have a unique User-ID and password (no User-ID sharing)
- Passwords should be a minimum of eight characters in length
- Passwords should be required to change periodically (60 days)
- Passwords should not be recycled less than six days
- Account lockout after five repeated failed login attempts

IDs that are not used for 90 days are deleted by the Corporate IT Operations Department. Also, default passwords for computers, network devices and software are disabled or changed to reduce risk of intrusion. Application systems authenticate users independently from the Operating System. Client administrators maintain the responsibility of managing user accounts for their organization. PeopleFluent requires a formal request from clients when adding, changing or removing client administrator's level of access. At VectorVMS, authorized VMS personnel utilize individual logins and passwords that grant administrator access to the Application. Each account gives personnel access to all utilities of the VMS Application.

Access Controls

After a user is successfully authenticated at the Operating System level, the user is assigned access privileges to the operating system, database, and application system functions. Authorized users access computer resources based upon approved user profiles that map resource access and system capabilities to their specific, assigned job functions.

VectorVMS will not allow client or client agents' access to sensitive system facilities unless a formal request from an authorized client contact is submitted. This includes access to the following:

- Program software libraries

- Test software libraries
- System administrative functions
- Application administrative functions
- Direct database access

Account Management

Upon receipt of a valid request from authorized Department Management personnel, Central IT Operations personnel are authorized to add, modify, or delete (disable) a VectorVMS corporate domain user account. Application user accounts for VectorVMS support users are administered by designated VMS Access administrators.

Client user accounts are administered by a specified client administrator. A client administrator is set up during the initial implementation by the Support Department. Clients submit a written request to change their administrator account information to the Support Department to reset passwords or change the account name. Before processing the change, the requesting party is validated through review of the listed client administrators and a support ticket is created.

For terminated VectorVMS employees, the HR Department completes a termination checklist and notifies the appropriate departments via email of the termination. PeopleFluent Security and Central IT Organization disables the employee’s password and corporate domain user logon IDs for network security. PeopleFluent Security receives a termination listing from HR and submits Account Deactivation request to the VMS Database Administration Team which develops a SQL script that is executed in the production, implementations, and disaster recovery environments to disable the terminated user’s account in VMS.

User profiles are updated for employees who change job functions to allow only those resources and capabilities required for the new position.

Upon receipt of a valid request to the VMS Access administrators, temporary unique user accounts are created granting access to client VMS implementations for troubleshooting and change request validations.

Administrative Accounts

Certain key administrative personnel within VectorVMS require system administration privileges to the operating, database and application systems. As stated above, these individuals are granted VMS administrator access on individual account IDs. Administrator activity is monitored as part of the auditing controls described above.

Consolidated Invoicing and Payment

VMS Consolidated Invoicing and Payment (CIP) is a product in which VectorVMS offers clients an option to receive one centralized invoice from VectorVMS on behalf of their contingent workforce suppliers tracking time through VMS. Per the contracted terms for VMS, VectorVMS is not obligated to pay supplier invoices until full payment has been received from the Client. Upon receipt of the full amount of the invoice, VectorVMS disburses the money due to the suppliers on behalf of the client, less a service fee retained by VectorVMS pursuant to the agreement between the Client and VectorVMS.

Integrations

As contractors are loaded into the VMS system and time is recorded for hours worked, an integration tool is used to perform the weekly transfer of the VMS information into Netsuite third-party billing software. From this integration, PeopleFluent performs the following services:

1. Applies sales tax as applicable per the supplier setup.
2. Creates a consolidated invoice for the client which contains information for all contracted employees per supplier for that week.

3. Creates multiple Accounts Payable invoices for each of the suppliers for amounts due upon receipt of payment from the client.
4. Records VectorVMS' service fees and any contracted client rebates for the week.

Invoicing

The consolidated invoice created from the integration is reviewed and compared to the VMS file for accuracy. The invoice is posted in the accounting system and is submitted to the client electronically.

Cash Receipts

There is a dedicated bank account and lockbox for the CIP clients to help ensure that funds are not intermingled with the operating funds for VectorVMS. VectorVMS requests payments to be made electronically, but if not, then secondarily submit a check to a lockbox. If payment does come to the corporate office, it is deposited by authorized Company personnel. Payments, electronic, lockbox or local, are posted in the accounting system by accounting personnel, who reviews a daily online printout of bank activity. As payments are submitted by the CIP client, they are applied to the invoice, and once it is paid in full, the Accounts Payable department is notified to release the payments due to the suppliers per the contracted terms. Additionally, bank reconciliations are performed monthly for the CIP bank account. Checks are color-coded by customer to further help ensure a proper matching of collections to vendor payments.

Cash Disbursements

CIP Vendor checks and Electronic Fund Transfers (EFT) are processed every Monday or Thursday. Authorized company personnel verify that checks from the client have cleared for payment to the vendors. The Accounting personnel create a check batch using a payables selection process which selects invoices for payment based on the PeopleFluent invoice number to the client. Next, the Accounting personnel reconcile the check batch total to the invoices sent to the client, less the contracted vendor discount. A secondary review of the reconciliation is performed by authorized Company personnel. The Accounting personnel review and electronically approve the resulting computer check edit report for disbursement. Additionally, the Assistant Controller generates the EFT file and it is transmitted to the bank.

Change Management

New releases and upgrades of application and database software are documented and tracked. The changes are tracked using the support ticketing system and the Production Change Board (PCB) calendar. Such changes are required to have approvals by the PCB which meets weekly to discuss production changes prior to implementation. The PCB reviews all proposed changes to production that are not Sev 1 changes and are not exempt based on risk assignment. The PCB charter describes in detail the types of changes that occur.

The Operations department performs operating system changes and tracks changes through the Google Workspace. All operating system changes are tested on the QA environment prior to being placed into production. All changes to code undergo peer review to help ensure appropriateness and accuracy. The peer reviews are documented and retained indefinitely to help ensure existence of the reviews. Before code is transferred between departments through the Production Change process, appropriate approvals should be documented.

VMS application requirements and specifications are created by Product Management. They are used by the Development and QA and Documentation teams to plan their work. The documents are used to define the new or changed functionality or infrastructural changes. Changes to the requirements/specifications are recorded and shared as appropriate.

Documentation and Procedure Updates

The individual analyst that is working on the change is responsible for updating the technical documentation in the support ticket as progress is achieved. The Support department supplies most significant documentation changes from a user perspective directly to the clients and retains technical documentation surrounding patches. For VectorVMS controlled software changes, the Development department updates the technical documentation as necessary.

Change Management items are tracked through the Production Change Board email accounts and the Engineer on call and Production Release email accounts. A record of everything that is moved and who actually performed the movement to production is saved in these accounts. The Production Change Board calendar records all releases going to the production environment. In addition, the CM team stores promotion packages promoted to the production environment in a network folder with read-only access. Only a member of the CM team has written access to this directory. The PCB is responsible for updating policies and procedures, as necessary, related to the Change Management issue.

Application Development and Maintenance

Application Development Personnel

There are two distinct groups in the Change Management process with the ability to develop and promote code into production. The development department is responsible for developing code. Once the code is developed, development personnel place the code on the development server to perform integration tests to test functionality. Once the code has successfully completed integration tests, the code is transferred to the control group. The development personnel do not have access to the code once the Control group acquires the code. The control group then moves the code to the QA environment where additional testing is performed. Once QA testing is complete, Software configuration management personnel use the build that was deployed to the QA environment as the basis for the release to be promoted to production. Operations will then promote this Configuration Management (“CM”) certified build to Staging where the Client Services organization performs client specific validation. Once staging testing is complete, the Operations promotes the CM certified build to production. If the code does not function properly, the process is restarted with the Development department redesigning the code.

Software Development Life Cycle (SDLC)

The VMS Application provides clients with billing information related to contingent labor provided by a variety of vendors. The VMS Application has the capability of providing billing information that can be integrated into the clients’ accounts payable systems and can also report accounts receivable information to vendors. Data exported from the VMS Application is complete and accurate to the extent that information is entered correctly by clients and vendors. VectorVMS achieves accuracy with respect to the financial data by providing controls around the QA environment where testing of the application is performed. When new versions, or builds, of the VMS Application are created, a series of tests in the QA and staging environments is applied to help ensure calculations, approvals and billing information are being accurately generated. The VMS QA department is a distinct group of individuals that performs testing. The QA team has no control over developing code or promoting code into production.

Prior to initiating the testing cycle, the Development team runs an extensive set of control tests cases to ensure quality of the build prior to deployment to QA. Once the control tests pass in the development control environment, QA request the promotion of code to the Quality environment. The QA team performs an initial quality test that checks basic functionality. This process is a form of baseline testing to help ensure primary functions are consistent with prior versions and functioning properly. If the build fails this test, it is transferred back to Development, along with documentation of errors, to correct the code and recycle through QA.

Once the build successfully passes the initial quality test, the QA team administers system integration test. The system integration test incorporates test cases that check scenarios that the VMS Application could experience, including different approvals, reports, rate changes and engagement alterations based on the scope of changes made during release cycle. This testing procedure includes manual testing. The QA team tests calculations performed by VMS manually. The QA team selects a sample of calculations to re-perform based on the characteristics of the new build and which clients will be affected by the new functionalities.

Test case failures are documented by the QA team. If a high severity failure is found by the QA team, the build is pushed back to Development; otherwise, the corrections are picked up by the QA team in subsequent builds. Testing results are documented in the qTest add-on for Jira which contains test cases, test plans and documentation on the progress of the tests. Subsequent to completion of the system integration test, the QA team administers new functionality testing. These test scripts focus on the new features of the release. New features that were not tested against the baseline scripts are tested to help ensure full functionality and accuracy of outputs. The test scripts that are deemed applicable are moved into system integration testing on the subsequent release and become part of residual testing. The last set of tests performed by the QA team is the regression suite, in which a modified component is tested in its fullest to validate that new functionality does not break existing functionality.

If there are client impacting changes and Product Management determines a staging period is required prior to Operations promoting the build into production, the build is placed in a staging environment, where the Client Services team performs client specific testing to validate the new functionality works as designed in a custom client environment. Partners and clients are encouraged to use the new release to gain comfort with the application and to identify potential errors. This process typically occurs two to three weeks prior to the Operations promoting the build into production.

Application Software Maintenance

The application software maintenance process is driven from different inputs, including new releases and patches from the Development department, as well as customer and internally generated Operations changes. The customer-driven change process commences with a request for specific work to be done by calling or accessing the support ticketing system which notifies VectorVMS' Support department of the Issue. This submission can come directly from a predefined customer administrator or an Account Manager (AM). AMs are assigned to premium customers that maintain a high volume of traffic on the VMS Application. Support inputs the request into the support ticketing system by creating an incident ticket. The support ticketing system is a third-party Customer Relations Management tool that tracks customer requests and incidents. For incidents that the Support personnel are unable to resolve, the employee escalates the incident ticket into an issue or Change Request ticket depending on the type of change. In addition, the Support personnel prioritize the requests, by assigning a severity level one through four, and then assigning the ticket to the appropriate department for resolution. There is an escalation protocol for Severity 1 issues contingent on the number of hours a request ticket is open. Support request tickets are categorized and processed according to the severity and SLA requirements. The following is the severity level table:

- Severity 1: Unable to use system - No workaround
- Severity 2: Critical issue to normal business operation - Operational issues - Core code defects
- Severity 3: Degraded Operations - Configuration defects - Core code defects
- Severity 4: Minimal impact

The tickets are sent to one contact in each department. Configuration changes are sent to the Professional Services team to develop a project estimate of time and cost. Programming changes are sent to either the Operations or Development departments depending on the type of change requested. Operations would answer the request if the programming issue related to the server or batch processes. Development would remediate the request if it related to software problems.

The support ticketing tool is used to log incidents from VMS and Consolidating Invoicing and Billing customers as well as sales and contact information. Unless otherwise specified herein, references to customers and clients are to the Company’s customers and clients for VMS and Consolidated Invoicing and Billing. The support ticketing system is password protected and is configurable to allow only certain groups access to functions of the tool. Individuals who perform any work related to a ticket insert a status update. The status updates log which individual performed the step and documents what has been performed to remediate the incident. The tickets also show the client contact, summary of issue and severity level. A new release of the support ticketing system allows clients to enter incidents directly into the support ticketing system via the support ticketing system. Clients are able to assign the incident a business impact level which will then be interpreted and assigned a Severity level by the personnel handling the issue. Clients also can review the status of their incidents through the support ticketing system.

Departmental Managers monitor their queues and upon receipt of the ticket, assign it to an analyst/programmer to review the change. After-hours’ requests and issues are handled by an on-call analyst/programmer from the Support department. The analyst/programmer is responsible for contacting the customer to confirm specific needs and for prioritizing the request. Specific information about work performed is documented within the support ticket. Should any work order fall under Change Management guidelines, it follows the Change Management process for approvals and execution.

Operations is responsible for database releases, hardware maintenance and upgrades, as well as operating system technical support and maintenance. The client or VectorVMS may initiate application software enhancements. Regardless of origin, changes are required to follow Change Management processes.

SLAs are observed with each client solution to determine resolution of problems. The status of incident tickets is communicated back to the client by the Support department or an AM as significant changes occur to the issues. Support or an AM attempts to contact the customer administrator three times subsequent to the resolution of a ticket. If no contact is made, the ticket is considered closed.

Job Scheduling

Job scheduling is an option for clients to download billing information from the VMS Application. Once selected, VectorVMS pushes the billing information to the secure File Transfer Protocol (FTP) server for its clients to download. The client is notified that the information has been distributed to the secure FTP server via email. FTP scripts are sent to the Support group to help ensure that complete and successful pushes occurred.

Operations logs and formal job scheduling are used. Job scheduling is performed using automated tools available on the different computing environments.

Computer Operations - Backups

US Operations

Policies and procedures are in place to describe the backup and recovery process. Database backups are scheduled and executed automatically at the primary US data center location. Scheduled tasks backup the Vendor Management System databases, files and other data from the Vendor Management System servers in the primary data center to the geographically diverse backup data center servers. Monitoring tools are in place to help ensure that the data is successfully backed-up and replicated to the secondary data center. Any backup exceptions are e-mailed to the Operations group to be resolved. Additionally, the backup personnel confirm execution of nightly backups by reviewing logs and determining whether there were exceptions. Backup tapes are generated from the backup data center and stored both on-site and off-site through a third-party vendor. Testing is performed regularly to help ensure data is recoverable.

Databases are subject to transaction logging, which provides a basis for recovery according to the sequence of operations performed against the database being re-sequenced in the event of an error. These transaction loggings are performed every 60 minutes.

Weekly backup tapes are stored off-site and maintained for six months. Monthly backups are taken off-site to Iron Mountain and maintained for thirteen months. Each group of tapes is secured in a container labeled with a barcode for tracking purposes. Backup utility software is used to track what information is contained on each tape. In order to restore a tape, personnel contact backup personnel and request a restored file. If the file was backed up within the previous week, on-site recovery is possible. If the recovered file was created prior to that, the PeopleFluent personnel notify the off-site storage vendor to retrieve a tape and deliver it to the secondary US data center facility. PeopleFluent uses a third-party off-site storage facility to maximize recovery of data. The storage facility maintains physical and environmental controls necessary to protect tapes. Physical security requirements include a visitor sign-in process, scheduled visits, visitor accompaniment and only designated personnel may request access to tapes.

UK Operations

Backups are scheduled and executed automatically at the UK data center location. Automated scheduled tasks initiate the backup process which copies the Vendor Management System databases, files and other system data from the Vendor Management System servers in Slough to a local backup server within the datacenter. Monitoring tools are in place to help ensure that the data is successfully backed-up. In the event of process exceptions, failure notifications are e-mailed to the Operations group for resolution. Additionally, the backup personnel confirm execution of nightly backups by reviewing logs and determining whether there were exceptions. Backup tapes are generated on-site and stored off-site with a third-party vendor as further described below.

Weekly backup tapes are stored off-site and maintained for six months. Monthly backups are taken off-site to Iron Mountain as well and are maintained for thirteen months. After backups are written to tape, Operations personnel enter a ticket with Cyxtera to take tape(s) from the tape library to a secure area to await pickup from the off-site storage company, Iron Mountain. A separate ticket is then entered with Iron Mountain to pick up the tape(s) from Cyxtera personnel. Both processes occur weekly and are tracked in the Cyxtera and Iron Mountain ticketing systems. The PeopleFluent requester is alerted if either of these steps is not performed by the appropriate party. The off-site storage company sends personnel to pick up the tape(s). Iron Mountain personnel are escorted while at the facility and do not have access to PeopleFluent cages. Each group of tapes is secured in a container labeled with a barcode for tracking purposes. Backup utility software is used to encrypt data as well as to track what information is contained on each tape. In order to restore a tape, requesters contact backup personnel to request restored data. If the file was backed up within the previous week, on-site recovery is possible. If the recovered file was created prior to that, the PeopleFluent personnel notify the off-site storage vendor to retrieve a tape and deliver it to the Cyxtera UK facility.

Canada Operations

Backups are scheduled and executed automatically at the Canadian data center location. Automated scheduled tasks initiate the backup process which copies Vendor Management System databases, files and other system data from the Vendor Management System servers to a local backup system within the datacenter. Monitoring tools are in place to help ensure that the data is successfully backed-up. In the event of process exceptions, failure notifications are e-mailed to the Operations group for resolution. Additionally, the backup personnel confirm execution of nightly backups by reviewing logs and determining whether there were exceptions. Backup tapes are generated on-site and stored off-site with a third-party vendor as further described below.

Weekly backup tapes are stored off-site and maintained for six months. Monthly backups are taken off-site to Iron Mountain as well and are maintained for thirteen months. After backups are written to tape, Operations personnel enter a ticket with Cyxtera to take tape(s) from the tape library to a secure area to await pickup from the off-site storage company, Iron Mountain. A separate ticket is then entered with Iron Mountain to pick up the tape(s) from Cyxtera personnel. Both processes occur weekly and are tracked in the Cyxtera and Iron Mountain ticketing systems. The PeopleFluent requester is alerted if either of these steps is not performed by the appropriate party. The off-site storage company sends personnel to pick up the tape(s). Iron Mountain personnel are escorted while at the facility and do not have access to PeopleFluent cages. Each group of tapes is secured in a container labeled with a barcode for tracking purposes. Backup utility software is used to encrypt data as well as to track what information is contained on each tape. In order to restore a tape, requesters contact backup personnel to request restored data. If the file was backed up within the previous week, on-site recovery is possible. If the recovered file was created prior to that, the PeopleFluent personnel notify the off-site storage vendor to retrieve a tape and deliver it to the Canadian data center facility.

Computer Operations - Availability

PeopleFluent utilizes a combination of custom developed and purchased applications to support the hosted provision of hosted Vendor Management System. A range of hardware platforms, operating systems, access mediums and delivery methods are supported, and customized solutions are available for most services, depending on customer requirements. The primary information systems and tools supporting PeopleFluent’s services are described below.

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

PeopleFluent monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLAs. PeopleFluent evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to the following:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth

PeopleFluent maintains an enterprise monitoring and ticketing application - an automated system that performs active checks on a preconfigured list of network segments, hosts, devices and services. Monitored attributes include availability of the network, host services and ports, IP packet transmissions and loss, bandwidth utilization and performance, Central Processing Unit (CPU) and hard disk utilization, temperature and cooling systems, power supply, voltage and redundancy. The application was designed as a complete solution for monitoring hardware, software, and environmental conditions, as well as tracking, escalating, and resolving incidents affecting PeopleFluent services.

Environmental monitoring - these monitoring systems provide audible and visual notification within the data center. The systems use devices throughout the facility to monitor air quality and smoke, temperature, humidity, and Uninterruptible Power Supply (UPS) capacity and availability.

Biometric and/or badge access system - physical access control systems that are linked to uniquely identifiable characteristics and personal information about the user. Employees and customers are required to enroll in the biometric security system database before accessing the PeopleFluent data center. Access activity is logged and associated with, biometric data (fingerprint geometry), and personal identification number used to gain or attempt access to the facility or data centers.

For specific controls implemented by Cyxtera, please refer to the ‘Subservice Organizations’ section below.

Data Transmission Security

Data transmissions between the client and the VMS Application are conducted in two different ways at the client’s option. The client pulls billing information from the VMS Application into its accounts payable system. This data can be downloaded from a Secure Sockets Layer (SSL) website or by pulling the information from a secured FTP server. VectorVMS offers the capability to PGP encrypt the data load for FTP and SFTP data exchanges. PeopleFluent runs batch jobs nightly that place billing information on the FTP server. The batch jobs are accompanied by e-mail notification to the client that the transfer was completed. FTP scripts are also e-mailed to the Support Department to help ensure that complete transfer of the data occurs. These scripts are monitored by Support personnel in the UK office where daily monitoring occurs. Data transmission also occurs between the VMS Application and the vendors that utilize the application. Vendors obtain receivables information from the application notifying them of their contractors’ billing information. The files are transferred via e-mails.

Boundaries of the System

The scope of this report includes the Vendor Management System performed in the Raleigh, North Carolina and Waltham, Massachusetts facilities.

This report does not include the colocation services provided by Cyxtera at the Atlanta, Georgia, Slough, United Kingdom, and Waltham, Massachusetts facilities, or the backup tape rotation and storage services provided by Iron Mountain.

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 VectorVMS’ control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of VectorVMS’ ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

Commitment to Competence

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

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

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

Management's Philosophy and Operating Style

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

Human Resources Policies and Practices

VectorVMS' 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 ensures the service organization is operating at maximum efficiency. VectorVMS' 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 employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

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

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

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

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

Integration with Risk Assessment

Along with assessing risks, VectorVMS 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 those objectives.

Information and Communications Systems

VectorVMS utilizes a combination of custom developed and purchased applications to support the data center hosting and managed services. A range of hardware platforms, operating systems, access mediums and delivery methods are supported, and customized solutions are available for most services, depending on customer requirements. The primary information systems and tools supporting VectorVMS' services are described below.

Enterprise monitoring and ticketing application - an automated system that performs active checks on a preconfigured list of network segments, hosts, devices and services. Monitored attributes include availability of the network, host services and ports, IP packet transmissions and loss, bandwidth utilization and performance, CPU and hard disk utilization, temperature and cooling systems, power supply, voltage and redundancy. The application was designed as a complete solution for monitoring hardware, software, and environmental conditions, as well as tracking, escalating, and resolving incidents affecting VectorVMS services.

Environmental monitoring - these monitoring systems provide audible and visual notification within the data center. The systems use devices throughout the facility to monitor air quality and smoke, temperature, humidity, and UPS capacity and availability.

Biometric and/or badge access system - physical access control systems that are linked to uniquely identifiable characteristics and personal information about the user. Employees and customers are required to enroll in the biometric security system database before accessing the PeopleFluent data center. Access activity is logged and associated with, biometric data (fingerprint geometry), and personal identification number used to gain or attempt access to the facility or data centers.

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

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate VectorVMS personnel via e-mail messages.

Monitoring Controls

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

On-Going Monitoring

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

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

Reporting Deficiencies

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

Changes to the System Since the Last Review

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/Security, Availability, Processing Integrity, and Confidentiality Criteria were applicable to VectorVMS' Vendor Management System.

Subservice Organizations

This report does not include the colocation services provided by Cyxtera at the Atlanta, Georgia, Slough, United Kingdom, and Waltham, Massachusetts facilities, or the backup tape rotation and storage services provided by Iron Mountain.

Complementary Subservice Organization Controls

VectorVMS/PeopleFluent'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 VectorVMS/PeopleFluent's services to be solely achieved by PeopleFluent control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of PeopleFluent.

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

Subservice Organization Controls - Cyxtera		
Category	**Criteria**	**Applicable Controls**
Common Criteria / Security	CC6.4	Security access controls (i.e., physical barriers and doors, card-control entry points, biometric scanning, video surveillance and /or manned reception desks) are utilized to protect areas that contain information and information processing facilities.
		Control mechanisms are in place to limit physical access to restricted areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.
		Data center badge access requests for Company employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.
		Data center access for Company personnel is revoked as a component of the termination process.
		Temporary access to the data centers for Company contractors must be pre-approved by a work order or ticket. Temporary access to data centers for customers requires prior authorization by the authorized customer representative.
		Customer maintained access lists are utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resides.
		Video logs are maintained for at least 90 days to document visitor activity at the data centers.
		Visitors are required to be escorted by an authorized Customer employee or authorized customer representative at all times while in the data centers.
		CCTV surveillance video and/or ACS activity log are retained for a minimum or 90 calendar days.

Subservice Organization Controls - Cyxtera		
Category	**Criteria**	**Applicable Controls**
		Data center security personnel and the PSCC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.
		An inventory of access badges and metal keys designated for loan to employees, customers, or contractors, as applicable by location, is performed at least once per day to account for all badges and metal keys.
		Badge access reviews are performed annually to help ensure that access to the data center facilities is restricted to authorized personnel.
Availability	A1.2	Environmental security policies and procedures are in place to guide personnel in the following areas: • Equipment specifications and operating instructions • Equipment inspections • Preventive maintenance schedules (internal and external maintenance activities)
		A BMS is configured to monitor data center equipment including, but not limited to, the following: • Fire detection and suppression systems, as applicable • HVAC units • Generators, as applicable • Electrical systems, as applicable
		The BMS is configured to notify data center staff via on-screen and e-mail alerts when predefined thresholds are exceeded on monitored devices.
		Power management equipment is in place at each data center.
		Third-party specialists inspect power management systems according to a predefined maintenance schedule.
		Fire detection and suppression equipment is in place at each data center.
		Third-party specialists inspect fire detection and suppression systems on an annual basis.
		HVAC systems are in place at each data center.
		Third-party specialists inspect HVAC systems and water detection sensors, as applicable, according to a predefined maintenance schedule.

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

Subservice Organization Controls - Iron Mountain		
Category	**Criteria**	**Applicable Controls**
Common Criteria / Security	CC6.4	Security access controls (i.e., physical barriers and doors, card-control entry points, biometric scanning, video surveillance and /or manned reception desks) are utilized to protect areas that contain information and information processing facilities.
		Control mechanisms are in place to limit physical access to restricted areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.
		Badge access requests for Company employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.
		Badge access for Company personnel is revoked as a component of the termination process.
		Temporary access to the data centers for Company contractors must be pre-approved by a work order or ticket. Temporary access to data centers for customers requires prior authorization by the authorized customer representative.
		Customer maintained access lists are utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resides.
		Video logs are maintained for at least 90 days to document visitor activity at the data centers.
		Visitors are required to be escorted by an authorized Customer employee or authorized customer representative at all times while in the data centers.
		CCTV surveillance video and /or ACS activity log are retained for a minimum or 90 calendar days.

VectorVMS/PeopleFluent 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, PeopleFluent 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
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

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

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the control objectives 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 VectorVMS.
2. User entities are responsible for notifying VectorVMS 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 PeopleFluent 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 VectorVMS services.
6. User entities are responsible for reconciling general ledger totals to Accounts Payable information to help ensure that information is completely and accurately updated.
7. User entities are responsible for reviewing reports on a timely basis to identify any processing errors and communicating any discrepancies to VectorVMS.
8. User entities are responsible for verifying that all data transmissions are completely obtained from the secured VectorVMS site.
9. User entities are responsible for configuring FTP software to communicate securely (SFTP) with the VectorVMS server.
10. User entities are responsible for verifying that time and expense information submitted by contractors is accurate before approving the reports.
11. User entities are responsible for verifying that all data have been entered completely, accurately and timely.
12. User entities are responsible for communicating contract and personnel changes to individuals authorized to use the VMS application that can appropriately update the information.
13. User entities are responsible for establishing individual user access rights within the VMS application.
14. User entities are responsible for performing regular user access reviews within the VMS application.
15. User entities are responsible for ensuring that personnel are properly trained in the use of the VMS application.
16. User entities are responsible for authorizing and approving all time and expense entries.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, Processing Integrity, and Confidentiality Categories)

Security refers to the protection of

1. information during its collection or creation, use, processing, transmission, and storage and
2. 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 services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of VectorVMS/PeopleFluent's description of the system. Any applicable trust services criteria that are not addressed by control activities at PeopleFluent are described within Section 4 and within the 'Subservice Organizations' and 'Criteria Not Applicable to the System' sections above.

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

SECTION 4

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

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

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

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, and the employee handbook.	Inspected the employee handbook to determine that core values were communicated from executive management to personnel through policies, directives, guidelines and the employee handbook.	No exceptions noted.
		Management has established a policy and procedure for reporting, handling and resolving complaints including violations of the code of conduct.	Inspected the employee handbook to determine that management had established a policy and procedure for reporting, handling and resolving complaints including violations of the code of conduct.	No exceptions noted.
		Personnel are provided a copy of the employee handbook, code of conduct and the statement of confidentiality and privacy practices upon hire.	Inspected the delivered policy documents for a sample of new hires to determine that personnel were provided a copy of the employee handbook, code of conduct and the statement of confidentiality and privacy practices upon hire.	No exceptions noted.
		Senior management has developed a background check policy to ensure individuals are being hired based on an acceptable background and skills requirements for the given position.	Inspected the background check policy to determine that senior management had developed a background check policy to ensure individuals were being hired based on an acceptable background and skills requirements for the given position.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to pass a criminal and financial trust background check upon being hired by the entity.	Inspected the completed background check for a sample of new hires to determine that personnel were required to pass a criminal and financial trust background check upon being hired by the entity.	No exceptions noted.
		Performance reviews are performed at least annually.	Inquired of the Chief Information Security Officer regarding the performance review process to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the employee performance review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the completed performance evaluation for a sample of current employees to determine that performance reviews were performed at least annually.	No exceptions noted.
		Management monitors compliance with training requirements.	Inspected the completed security awareness training report for a sample of current employees to determine that management monitored compliance with training requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
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 maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and internal controls matrix to determine that executive management-maintained independence from those that operate the key controls within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the executive management meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls 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**
			Inspected meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
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 to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed annually by management.	Inspected the organizational chart to determine that the reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected the job description for a sample of job roles to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected job descriptions for a sample of job roles to determine roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected the job description for a sample of job roles to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Performance reviews are performed at least annually.	Inquired of the Chief Information Security Officer regarding the performance review process to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the employee performance review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the completed performance evaluation report for a sample of current employees to determine that performance reviews were performed at least annually.	No exceptions noted.
		Personnel are required to take an annual information security training.	Inquired of the Chief Information Security Officer regarding the communication of security, availability, processing integrity and confidentiality commitments to determine that personnel were required to take an annual information security training.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Control Environment</th></tr>
<tr><th>CC1.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the completed security awareness report for a sample of current employees to determine that personnel were required to take an annual information security training.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Management establishes skills and continued training with its commitments and requirements for employees.</td><td>Inspected the security awareness training materials and the LMS to determine that management established skills and continued training with its commitments and requirements to employees.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Management monitors compliance with training requirements.</td><td>Inspected the security awareness training completion report to determine that management monitored compliance with training requirements.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Personnel are required to pass a criminal and financial trust background check upon being hired by the entity.</td><td>Inspected the completed background check for a sample of new hires to determine that personnel were required to pass a criminal and financial trust background check upon being hired by the entity.</td><td>No exceptions noted.</td></tr>
<tr><td>CC1.5</td><td>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</td><td>A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.</td><td>Inspected the organizational chart to determine that a documented organizational chart was in place to assign responsibility and delegate lines of authority to personnel.</td><td>No exceptions noted.</td></tr>
</table>

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 managers and their supervisors.	Inquired of the Chief Information Security Officer regarding the organizational structure to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted.
			Inspected job description for a sample of job roles to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions.	Inspected job description for a sample of job roles to determine that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Personnel are provided a copy of the employee handbook, code of conduct and the statement of confidentiality and privacy practices upon hire.	Inspected the delivered policy documents for a sample of new hires to determine that personnel were provided a copy of the employee handbook, code of conduct and the statement of confidentiality and privacy practices upon hire.	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 reviews are performed at least annually.	Inquired of the Chief Information Security Officer regarding the performance review process to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the employee performance review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the completed performance evaluation report for a sample of current employees to determine that performance reviews were performed at least annually.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Information and Communication</th></tr>
<tr><th>CC2.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>CC2.1</td><td>COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</td><td>Policies and procedures are documented for significant processes are available on the entity’s intranet.</td><td>Observed policies on the company intranet to determine that policies and procedures were documented for significant processes were available on the entity’s intranet.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the entity’s policies and intranet to determine that policies and procedures were documented for significant processes were available on the entity’s intranet.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.</td><td>Inspected the data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.</td><td>No exceptions noted.</td></tr>
<tr><td>CC2.2</td><td>COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</td><td>Security, availability, processing integrity, and confidentiality commitments are communicated to external users via SLAs.</td><td>Inspected the entity website and the SLA for a sample of customers to determine that security, availability, processing integrity, and confidentiality commitments were communicated to external users via defined SLAs.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Policies and procedures are documented for significant processes are available on the entity’s intranet.</td><td>Observed policies on the company intranet to determine that policies and procedures were documented for significant processes were available on the entity’s intranet.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's policies and intranet to determine that policies and procedures were documented for significant processes were available on the entity's intranet.	No exceptions noted.
		Personnel are provided a copy of the employee handbook, code of conduct and the statement of confidentiality and privacy practices upon hire.	Inspected the delivered policy documents for a sample of new hires to determine that personnel were provided a copy of the employee handbook, code of conduct and the statement of confidentiality and privacy practices upon hire.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions.	Inspected job description for a sample of job roles to determine that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
		Management makes updates to job descriptions when necessary.	Inspected revision date for a sample of job descriptions to determine that management made updates to job descriptions when necessary.	No exceptions noted.
		Personnel are required to take an annual information security training.	Inquired of the Chief Information Security Officer regarding the communication of security, availability, processing integrity and confidentiality commitments to determine that personnel were required to take an annual information security training.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed security awareness report for a sample of current employees to determine that personnel were required to take an annual information security training.	No exceptions noted.
		Customer responsibilities are outlined and communicated through SLAs.	Inspected the SLA for a sample of customers to determine that customer responsibilities were outlined and communicated through SLAs.	No exceptions noted.
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
		The organization's security policies and code of conduct are communicated to employees in the employee handbook.	Inspected the information security policy and employee handbook to determine that the organization's security policies and code of conduct were communicated to employees in the employee handbook.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	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**
		Defined SLAs are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security, availability, processing integrity, and confidentiality related failure, incidents, and concerns to personnel.	Inspected the SLA for a sample of customers to determine that defined SLAs were in place and communicated to authorized external users. The SLAs included communication procedures for reporting security, availability, processing integrity, and confidentiality related failure, incidents, and concerns to personnel.	No exceptions noted.
		The functional vice president (VP) is responsible for changes to confidentiality practices and commitments.	Inspected the confidentiality practices and commitments change policy to determine that the functional VP was responsible for changes to confidentiality practices and commitments.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the executive meeting minutes and PowerPoint 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.

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**
		A formal process is used to communicate confidentiality changes to users, related parties, and vendors.	Inquired of the Chief Information Security Officer regarding the communication of confidentiality commitments to determine that a formal process was used to communicate confidentiality changes to users, related parties, and vendors.	No exceptions noted.
			Inspected the confidentiality practices and commitments change policy to determine that a formal process was used to communicate confidentiality changes to users, related parties, and vendors.	No exceptions noted.
		The company has a contract in place with outsourced data center providers which requires a third-party audit that includes physical security.	Inspected the third-party contracts and the completed SOC report to determine that the company had a contract in place with outsourced data center providers which required a third-party audit that included physical security.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	System descriptions are communicated to authorized external users via SLA that delineate the boundaries of the system and describe relevant system components.	Inspected the master SLA to determine that system descriptions were communicated to authorized external users via SLA that delineated the boundaries of the system and describe 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**
			Inspected the SLA for a sample of customers to determine that system descriptions were communicated to authorized external users via SLA that delineated the boundaries of the system and describe relevant system components.	No exceptions noted.
		A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel.	Inspected the policies and procedures posted to the intranet to determine that a description of the system delineating the boundaries of the system was posted on a secure network drive and was available to personnel.	No exceptions noted.
		Customer responsibilities are outlined and communicated through SLAs.	Inspected the SLA for a sample of customers to determine that customer responsibilities were outlined and communicated through SLAs.	No exceptions noted.
		Security, availability, processing integrity, and confidentiality commitments are communicated to external users via defined SLA.	Inspected the SLA for a sample of customers to determine that security, availability, processing integrity, and confidentiality commitments were communicated to external users via defined SLA.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Observed policies on the company intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected entity policies to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Defined SLAs are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security, availability, processing integrity, and confidentiality related failure, incidents, and concerns to personnel.	Inspected the SLA for a sample of customers to determine that defined SLAs were in place and communicated to authorized external users. The SLAs included communication procedures for reporting security, availability, processing integrity, and confidentiality related failure, incidents, and concerns to personnel.	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 functional VP is responsible for changes to confidentiality practices and commitments.	Inspected the confidentiality practices and commitments change policy to determine that the functional VP was responsible for changes to confidentiality practices and commitments.	No exceptions noted.
		A formal process is used to communicate confidentiality changes to users, related parties, and vendors.	Inquired of the Chief Information Security Officer regarding the communication of confidentiality commitments to determine that a formal process was used to communicate confidentiality changes to users, related parties, and vendors.	No exceptions noted.
			Inspected the confidentiality practices and commitments change policy to determine that a formal process was used to communicate confidentiality changes to users, related parties, and vendors.	No exceptions noted.
		The company has a contract in place with outsourced data center providers which requires a third-party audit that includes physical security.	Inspected the third-party contracts and the completed SOC report to determine that the company had a contract in place with outsourced data center providers which required a third-party audit that included physical security.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, employee performance policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected executive management meeting minutes and the associated PowerPoint deck 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.
		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 and the entity's documented objectives and strategies 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.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Risk Assessment</th></tr>
<tr><th>CC3.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Executive management reviews operational and resourcing reports to evaluate performance and resourcing at least annually.</td><td>Inspected executive management meeting minutes and the associated PowerPoint deck to determine that executive management reviewed operational and resourcing reports to evaluate performance and resourcing at least annually.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Business plans and budgets align with the entity's strategies and objectives.</td><td>Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>The operational reports reviewed by executive management define the acceptable level of operational performance and control failure.</td><td>Inspected operational reports to determine that the operational reports reviewed by executive management defined the acceptable level of operational performance and control failure.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.</td><td>Inspected the internal controls matrix, 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.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Applicable law, regulation, standard, and legislature requirements are identified and integrated into the entity's strategies and objectives.	Inspected the entity's documented objectives and strategies and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine applicable law, regulation, standard, and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing the risk assessment process.	No exceptions noted.
		The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the completed risk assessment to determine that the entity had defined a formal risk management process that specified the risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		During the risk assessment and management process, risk management office personnel identify risk scenarios that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the completed risk assessment to determine that during the risk assessment and management process, risk management office personnel identified risk scenarios that threatened the achievement of business objectives and updated the potential threats to system 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**
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	Inspected the risk assessment and management policies and procedures to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.
			Inspected the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.
		Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inquired of the VP of Hosting Systems and Operations regarding the risk management process to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
			Inspected the risk assessment policy to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	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 risk and compliance meeting minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed fraud assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.

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

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 key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Risk Assessment</th></tr>
<tr><th>CC3.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>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.</td><td>No exceptions noted.</td></tr>
</table>

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, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring system configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, 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 system configurations, notification configurations and an example alert to determine that the monitoring software was configured to IT personnel when thresholds had been exceeded.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inspected the incident response policy and procedures to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
		An external vulnerability assessment is performed at least annually by an independent vendor to identify vulnerabilities in the network.	Inspected the completed external vulnerability scan assessment to determine that an external vulnerability assessment was performed at least annually by an independent vendor to identify vulnerabilities in the network.	No exceptions noted.
		A formal risk assessment is performed annually basis to identify threats that could impair systems security, availability, processing integrity, and confidentiality commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed annually to identify threats that could impair systems security, availability, processing integrity, and confidentiality 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**
		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 review for a sample of third-parties that the entity has a relationship with 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.
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.	Inquired of the VP of Hosting Systems and Operations regarding the risk management process to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
			Inspected the risk assessment policy to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
			Inspected the risk and compliance meeting minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the vulnerability tracking dashboard and tickets for an example vulnerability to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the annual risk assessment are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment and vulnerability scan results to determine that vulnerabilities, deviations, and control gaps identified from the annual risk assessment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the associated incident ticket for an example internal control that has failed to determine that vulnerabilities, deviations, and control gaps identified from the annual risk assessment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for an example vulnerability from the vulnerability scan results to determine that vulnerabilities, deviations, and control gaps identified from the annual risk assessment 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**
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring system configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert the senior security analyst when thresholds have been exceeded.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that the monitoring software was configured to alert the senior security analyst when thresholds had been exceeded.	No exceptions noted.
		A formal risk assessment is performed annually basis to identify threats that could impair systems security, availability, processing integrity, and confidentiality commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed annually to identify threats that could impair systems security, availability, processing integrity, and confidentiality commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy and completed risk assessment to determine that management defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the internal controls matrix to determine 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.
		An external vulnerability assessment is performed at least annually by an independent vendor to identify vulnerabilities in the network.	Inspected the completed external vulnerability scan assessment to determine that an external vulnerability assessment was performed at least annually by an independent vendor to identify vulnerabilities in the network.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery plan to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy and the completed risk assessment to determine that management defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	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.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans, including restoration of backups, were tested annually.	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**
		An external vulnerability assessment is performed at least annually by an independent vendor to identify vulnerabilities in the network.	Inspected the completed external vulnerability scan assessment to determine that an external vulnerability assessment was performed at least annually by an independent vendor to identify vulnerabilities in the network.	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.	Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected the job description for a sample of job roles to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the internal controls matrix to determine 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.
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected the internal controls matrix and the entity’s attestation report 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.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Inspected the master list of system components to determine that a master list of the entity's system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted.
		Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the information security policy, e-mail notification and supporting user access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical and physical access to systems is revoked as a component of the termination process.	Inspected the information security policy, supporting termination checklist, HR separation e-mail, badge access listing, and Windows domain account status for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights and the termination listing 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 user accounts accessible by authorized personnel.	Inquired of the Chief Information Security Officer regarding administrative access to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by 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**
		Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Minimum password length • Password complexity • Password expiration • Password history • Invalid attempt lockout	Inspected the network authentication settings to determine that network users were authenticated via individually-assigned user accounts and passwords. Networks were configured to enforce password requirements that included: • Minimum password length • Password complexity • Password expiration • Password history • Invalid attempt lockout	No exceptions noted.
		Network account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout policy to determine that network account lockout policies 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 policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging policy to determine that network audit policy configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Alerts are generated to notify network administrators of suspicious activity.	Inspected the network monitoring configurations and a sample network alert to determine that alerts were generated to notify network administrators of suspicious activity.	No exceptions noted.
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database administrator listing and to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Chief Information Security Officer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Database users are authenticated via individually-assigned user accounts and passwords. Databases are configured to enforce password requirements that include: • Password length • Complexity	Inspected the database authentication settings to determine that database users were authenticated via individually-assigned user accounts and passwords. Databases were configured to enforce password requirements that included: • Password length • Complexity	No exceptions noted.
		Database audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the database audit logging settings to determine that database audit policy configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Alerts are generated to notify database administrators of suspicious activity.	Inspected a sample database alert and the notification configurations to determine that alerts were generated to notify database administrators of suspicious activity.	No exceptions noted.
		Virtual Private Network (VPN) user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to user accounts accessible by authorized personnel.	Inquired of the Chief Information Security Officer regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		External access by employees is permitted only through a two-factor encrypted VPN connection.	Inquired of the Chief Information Security Officer regarding logical access security software to determine that external access by employees was permitted only through a two-factor encrypted VPN connection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Observed a user log into the VPN to determine that external access by employees was permitted only through two-factor encrypted VPN connection.	No exceptions noted.
			Inspected the two-factor remote access authentication settings to determine that external access by employees was permitted only through a two-factor encrypted VPN connection.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication (username, password, and OTP) prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication (username, password, and OTP) prior to being granted remote access to the system.	No exceptions noted.
		Privileged access to sensitive resources is restricted to defined user roles.	Inspected the user access listings and access rights to determine that privileged access to sensitive resources were restricted to defined user roles.	No exceptions noted.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the Demilitarized Zone (DMZ) settings to determine the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine a DMZ was in place to isolate outside access and data from the entity's 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**
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the TLS certificate to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Stored passwords are encrypted.	Inspected encryption configurations for data at rest to determine that stored passwords were encrypted.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the information security policy, e-mail notification and supporting user access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical and physical access to systems is revoked as a component of the termination process.	Inspected the information security policy, supporting termination checklist, HR separation e-mail, badge access listing, and Windows domain account status for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Account sharing is prohibited unless a variance from policy is granted by the Chief Information Security Officer.	Inspected the information security policy to determine that account sharing was prohibited unless a variance from policy was granted by the Chief Information Security Officer.	No exceptions noted.
		Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the information security policy, e-mail notification and supporting user access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical and physical access to systems is revoked as a component of the termination process.	Inspected the information security policy, supporting termination checklist, HR separation e-mail, badge access listing, and Windows domain account status for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Policies and procedures are in place to guide personnel in physical security activities.	Inspected the physical security policy to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
		A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.	Observed the entrance to the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
		A badge access system controls access to and within the office facility.	Observed the presence of badge access points within the facility to determine that a badge access system-controlled access to and within the office facility.	No exceptions noted.
			Inspected the badge access listing and zone definitions to determine that a badge access system-controlled access to and within the office facility.	No exceptions noted.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.	Inspected the badge access listing and zone definitions to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.	No exceptions noted.
		Inspected the badge access configurations and the oldest badge access log to determine that the badge access system logged successful and failed access attempts, and that the logs could be pulled for review if necessary.	Inspected the badge access configurations and the oldest badge access log to determine that the badge access system logged successful and failed access attempts, and that the logs could be pulled for review if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to request badge access changes is restricted to user accounts accessible by authorized personnel.	Inquired of the Chief Information Security Officer regarding administrative access to determine that the ability to request badge access changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the badge access administrator listing to determine that the ability to request badge access changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the information security policy, e-mail notification and supporting user access request ticket for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
		Access to the server room is restricted to badge access cards assigned to authorized personnel.	Inquired of the Chief Information Security Officer regarding administrative access to determine that access to the server room was restricted to badge access cards assigned to authorized personnel.	No exceptions noted.
			Inspected the badge access listing and zone definitions to determine that access to the server room was restricted to badge access cards assigned 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 video surveillance system is in place with footage retained for 30 days.	Inspected surveillance footage to determine that a video surveillance system was in place with footage retained for 30 days.	No exceptions noted.
		Visitors to the facility and server room are required to be escorted by an authorized employee.	Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.
			Inspected the physical security policy to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.
		Visitors to the facility and server room are required to sign a visitor log upon arrival.	Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to sign a visitor log upon arrival.	No exceptions noted.
			Inspected the visitor sign in log for a sample of weeks to determine that visitors to the facility and server room were required to sign a visitor log upon arrival.	No exceptions noted.
		Physical access privileges to the corporate office facility are revoked as a component of the termination process.	Inspected the information security policy, supporting termination checklist for a sample of terminated employees, and badge access user listing to determine that physical access privileges to the corporate office facility were revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		User access to the badge access system is reviewed on an annual basis.	Inspected the completed badge access audit to determine that user access to the badge access system was reviewed on an annual basis.	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.
CC6.5	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.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
		The entity purges data stored on backup tapes and backup drives when no longer needed for business purposes.	Inspected the vendor provided media destruction report to determine that the entity purged data stored on backup tapes and backup drives when no longer needed for business purposes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data that is no longer required for business purposes is rendered unreadable.	Inspected the data disposal and destruction policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the supporting service ticket for a sample of requests to dispose of data, purge a system, or physically destroy a system, to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall rule set 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 rule set to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Antivirus protection is installed on Windows based servers and workstations and updates are applied as released to protect company data from infection by malicious code or virus.	Inquired of the Chief Information Security Officer regarding antivirus protection on workstations to determine that antivirus protection was installed on Windows based servers and workstations and updates were applied as released to protect company data from infection by malicious code or virus.	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 antivirus configuration settings to determine that antivirus protection was installed on Windows based servers and workstations and updates were applied as released to protect company data from infection by malicious code or virus.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus scan settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		The antivirus software provider pushes updates to the installed anti-virus software as new updates/signatures are available.	Inspected the antivirus update settings to determine that the antivirus software provider pushed updates to the installed anti-virus software as new updates/signatures are available.	No exceptions noted.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		Remote connectivity users are authenticated via multi-factor authentication before establishing a VPN session.	Observed a user authenticate into the VPN to determine that remote connectivity users were authenticated via multi-factor authentication before establishing a VPN session.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via multi-factor authentication before establishing a VPN session.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS notification configurations to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
			Inspected a sample intrusion alert to determine that the IDS was configured to notify the security team upon intrusion detection.	No exceptions noted.
		Application security restricts output to approved roles or user IDs.	Inquired of the Chief Information Security Officer regarding application security to determine that application security restricted output to approved roles or user IDs.	No exceptions noted.
			Inspected the VMS user listing, network administrative listing, database administrator listing, VPN administrator listing, and the application authentication configuration to determine that application security restricted output to approved roles or user IDs.	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**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the TLS certificate to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system occurs through the use authorized software supporting the Advanced Encryption Standard (AES).	Inspected file encryption configurations and the encryption policies to determine that transmission of digital output beyond the boundary of the system occurred through the use authorized software supporting the AES.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the Acceptable Use Policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected removable media configurations to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	VPN and TLS technologies are used for defined points of connectivity.	Inspected the VPN configuration, TLS certificates and encryption policy to determine that VPN and TLS were used for defined points of connectivity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Backup media is stored in an encrypted format.	Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Backup media is rotated off-site by a third-party vendor on a biweekly basis.	Inspected the contract in place with the offsite storage vendor and a log of backup rotations for a sample of weeks to determine that backup media was rotated off-site by a third-party vendor on a biweekly basis.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the vendor provided listing of users with the ability to recall backup media to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Chief Information Security Officer regarding the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listing of users with access to 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.
		An external vulnerability assessment is performed at least annually by an independent vendor to identify vulnerabilities in the network.	Inspected the completed external vulnerability scan assessment to determine that an external vulnerability assessment was performed at least annually by an independent vendor to identify vulnerabilities in the network.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS notification configurations to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
			Inspected a sample intrusion alert to determine that the IDS was 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**
		Antivirus protection is installed on Windows based servers and workstations and updates are applied as released to protect company data from infection by malicious code or virus.	Inquired of the Chief Information Security Officer regarding antivirus protection on workstations to determine that antivirus protection was installed on Windows based servers and workstations and updates were applied as released to protect company data from infection by malicious code or virus.	No exceptions noted.
			Inspected the antivirus configuration settings to determine that antivirus protection was installed on Windows based servers and workstations and updates were applied as released to protect company data from infection by malicious code or virus.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus scan settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		The antivirus software provider pushes updates to the installed anti-virus software daily.	Inspected the antivirus update settings to determine that the antivirus software provider pushed updates to the installed anti-virus software daily.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring system configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, 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 system configurations, notification configurations and a sample alert to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS notification configurations to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
			Inspected a sample intrusion alert to determine that the IDS was configured to notify the security team 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**
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.	An external vulnerability assessment is performed at least annually by an independent vendor to identify vulnerabilities in the network.	Inspected the completed external vulnerability scan assessment to determine that an external vulnerability assessment was performed at least annually by an independent vendor to identify vulnerabilities in the network.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring system configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, 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 system configurations, notification configurations and a sample alert to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	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 automated backup system is utilized to perform scheduled system backups.	Inspected the backup system configurations to determine that an automated backup system was utilized to perform scheduled system backups.	No exceptions noted.
		Full backups of certain application and database components are performed on a weekly basis and incremental backups are performed on a nightly basis.	Inspected the backup configurations and a sample of backup logs to determine that full backups of certain application and database components were performed on a weekly basis and incremental backups were performed on a nightly basis.	No exceptions noted.
		IT personnel monitor the success or failure of backups and are notified of backup job status via e-mail notifications.	Inquired of the Chief Information Security Officer regarding the monitoring of system backups to determine that IT personnel monitored the success or failure of backups and were notified of backup job status via e-mail notifications.	No exceptions noted.
			Inspected the backup notification configurations, backup status alert, and the completed backup jobs for a sample of days to determine that IT personnel monitored the success or failure of backups and were notified of backup job status via e-mail notifications.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software.	Inquired of the Chief Information Security Officer regarding antivirus protection on workstations to determine that antivirus protection was installed on Windows based servers and workstations and updates were applied as released to protect company data from infection by malicious code or virus.	No exceptions noted.
			Inspected the antivirus configuration settings to determine that antivirus protection was installed on Windows based servers and workstations and updates were applied as released to protect company data from infection by malicious code or virus.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus scan settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		The antivirus software provider pushes updates to the installed anti-virus software as new updates/signatures are available.	Inspected the antivirus update settings to determine that the antivirus software provider pushes updates to the installed anti-virus software as new updates/signatures are available.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall rule set to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule set 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 is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS notification configurations to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
			Inspected a sample intrusion alert to determine that the IDS was configured to notify the security team upon intrusion detection.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents.	Inspected the supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Resolution of incidents is communicated to users within the corresponding ticket.	Inspected the supporting ticket for a sample of incidents to determine that resolution of incidents was communicated to users within the corresponding ticket.	No exceptions noted.
		Change management requests are opened for events that require permanent fixes.	Inspected the supporting ticket for a sample of system changes to determine that change management requests were opened for events that required permanent fixes.	No exceptions noted.
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	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**
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inspected the incident response policy and procedures to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident management and escalation policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, including business impact and response time frame.	Inspected incident management reports to determine that management reviewed reports on an annual basis summarizing incidents, including business impact and response time frame.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents.	Inspected the supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.
		Resolution of incidents is communicated to users within the corresponding ticket.	Inspected the supporting ticket for a sample of incidents to determine that resolution of incidents was communicated to users within the corresponding ticket.	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**
		Change management requests are opened for events that require permanent fixes.	Inspected the supporting ticket for a sample of system changes to determine that change management requests were opened for events that required permanent fixes.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents.	Inspected the supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.
		Resolution of incidents is communicated to users within the corresponding ticket.	Inspected the supporting ticket for a sample of incidents to determine that resolution of events was communicated to users within the corresponding ticket.	No exceptions noted.
		Change management requests are opened for events that require permanent fixes.	Inspected the supporting ticket for a sample of system changes to determine that change management requests were opened for events that required permanent fixes.	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews reports on an annual basis summarizing incidents, including business impact and response time frame.	Inspected management reports to determine that management reviews reports on an annual basis summarizing incidents, including business impact and response time frame.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the handling system changes.	Inspected the change control policies and procedures to determine that documented change control procedures were in place to guide personnel in the handling of system changes.	No exceptions noted.
		System changes are authorized, tested, and approved by management prior to implementation.	Inspected the supporting ticket for a sample of system changes to determine that system changes were authorized, tested, and approved by management prior to implementation.	No exceptions noted.
		Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented escalation procedures for reporting security incidents were in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents.	Inspected the supporting ticket for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.
		Change management requests are opened for events that require permanent fixes.	Inspected the supporting ticket for a sample of system changes to determine that change management requests were opened for events that required permanent fixes.	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 changes are communicated to both internal and external users.	Inspected e-mail communication to internal and external users to determine that system changes were communicated to both internal and external users.	No exceptions noted.
		QA environments are physically and logically separated from the production environment.	Inspected the QA and production server listings to determine that QA environments were physically and logically separated from the production environment.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Chief Information Security Officer regarding access to implement changes into production to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
			Inspected the listing of users with access to make changes in development and deploy changes into production to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The change management process has defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-QA department • Implementation software change management group	Inspected the change control policies and procedures, supporting ticket for a sample of changes to determine that the change management process had defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-QA department • Implementation software change management group	No exceptions noted.
		The entity creates test data using data masking software that replaces confidential information with test information prior to the creation of test databases.	Inspected the data masking software to determine that the entity created test data using data masking software that replaced confidential information with test information prior to the creation of test databases.	No exceptions noted.
		Management has defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management had defined configuration standards in the information security policies and procedures.	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**
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the information security policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing the risk assessment process.	No exceptions noted.
		The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the completed risk assessment to determine that the entity had defined a formal risk management process that specified the risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		A formal risk assessment is performed annually to identify threats that could impair systems security, availability, processing integrity, and confidentiality commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed annually to identify threats that could impair systems security, availability, processing integrity, and confidentiality commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and rating are reviewed by management.	Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address all 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**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
		Security and confidentiality commitments regarding the system are included in related party and vendor specific SLAs.	Inspected the third-party contracts and the completed SOC reports to determine that security and confidentiality commitments regarding the system were included in related party and vendor specific SLAs.	No exceptions noted.
		The company has a contract in place with outsourced data center providers which requires a third-party audit that includes physical security.	Inspected the third-party contracts and the completed SOC report to determine that the company had a contract in place with outsourced data center providers which required a third-party audit that included physical security.	No exceptions noted.
		The entity's third-party agreements outline and communicate the terms, conditions and responsibilities of third-parties.	Inspected the vendor onboarding procedures and agreement for a sample of third-parties to determine that the agreements outlined and communicated the terms, conditions and responsibilities of 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 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 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.
		The entity's third-party agreement outlines and communicates confidentiality commitments and requirements.	Inspected the vendor onboarding procedures and agreement for a sample of third-parties to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS alert configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the system monitoring software configuration and a sample alert notification to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the system monitoring software configuration and a sample system monitoring log to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
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.	Management has contracted with a third-party data center to provide secure hosting of production systems and data.	Inspected the contract in place with the third-party data center to determine that management had contracted with a third-party data center to provide secure hosting of production systems and data.	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**
		Full backups of application and database components are performed on a weekly basis and incremental backups are performed on a daily basis.	Inspected the backup configurations and a sample of backup logs to determine that full backups of certain application and database components were performed on a weekly basis and incremental backups were performed on a nightly basis.	No exceptions noted.
		IT personnel monitor the success or failure of backups and are notified of backup job status via e-mail notifications.	Inquired of the Chief Information Security Officer regarding the monitoring of system backups to determine that IT personnel monitored the success or failure of backups and were notified of backup job status via e-mail notifications.	No exceptions noted.
			Inspected the backup notification configurations, backup status alert, and the completed backup jobs for a sample of days to determine that IT personnel monitored the success or failure of backups and were notified of backup job status via e-mail notifications.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Backup media is rotated off-site by a third-party vendor on a biweekly basis.	Inspected the contract in place with the offsite storage vendor and a log of backup rotations for a sample of weeks to determine that backup media was rotated off-site by a third-party vendor on a biweekly 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**
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the vendor provided listing of users with the ability to recall backup media to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	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.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery plan to determine that a disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	No exceptions noted.
			Inspected the completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY				
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	Data flow diagrams are documented and maintained by management to identify the critical data points and flow of information.	Inspected data flow diagrams to determine that data flow diagrams were 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 is critical to support the system.	Inspected 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 data classification policy to determine that the entity 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	No exceptions noted.
		Management reviews the inventory of data and information that is critical to support the system for completeness and accuracy.	Inspected the data assessment dashboard to determine that management reviewed the inventory of data and information that is critical to support the system for completeness and accuracy.	No exceptions noted.
		Data is classified and structured in a consistent manner.	Inspected the data classification policy and the database 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 entity has established data preparation procedures to be followed by user departments and customers.	Inspected the data classification policy to determine that the entity had established data preparation procedures that were followed by user departments and customers.	No exceptions noted.
		The types of information input into the system by user entities is defined and documented.	Inspected the information security policies to determine that the types of information input into the system by user entities was defined and documented.	No exceptions noted.
		System edits are completed before record entry is accepted.	Observed personnel incorrectly entering information into the VMS application to determine that system edits were completed before record entry was accepted.	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.	Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the system monitoring software configuration and a sample alert notification to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the system monitoring software configuration and a sample system monitoring log to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
		The entity has defined what critical data is processed and how it is processed.	Inspected the information security policies to determine that the entity has defined what critical data is processed and how it is 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.	Applications are configured to process output data and reports completely, accurately, timely and only to authorized users.	Inquired of the Chief Information Security Officer regarding system output to determine that applications were configured to process output data and reports completely, accurately, timely and only to authorized users.	No exceptions noted.
			Inspected the production applications security settings and user access control list to determine that applications were configured to process output data and reports completely, accurately, timely and only to authorized users.	No exceptions noted.
		System edits are completed before record entry is accepted.	Observed personnel incorrectly entering information into the VMS application to determine that system edits were completed before record entry was accepted.	No exceptions noted.
		Application security restricts output to approved user IDs.	Inspected the production applications security settings and user access control list to determine that application security restricted output to approved user IDs.	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.	Critical data output from the system is stored and transmitted using secure encryption methods.	Inspected encryption configurations for data in transit and digital certificates to determine that critical data output from the system was stored and transmitted using secure encryption methods.	No exceptions noted.
		Procedures are in place to provide for the completeness, accuracy, and timeliness of critical data that is output from the system.	Inspected the information security policies to determine that procedures were in place to provide for the completeness, accuracy, and timeliness of critical data that was output from the system.	No exceptions noted.
		Backups are performed using an automated backup system.	Inspected the backup system configuration to determine that backups were performed using an automated backup system.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Backup media is rotated off-site by a third-party vendor on a biweekly basis.	Inspected the contract in place with the offsite storage vendor and a log of backup rotations for a sample of weeks to determine that backup media was rotated off-site by a third-party vendor on a biweekly basis.	No exceptions noted.
		Procedures are in place to provide for complete, accurate, and timely storage of data.	Inspected information security policies to determine that procedures were in place to provide for complete, accurate, and timely storage of 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**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The entity establishes written policies related to retention periods for the confidential information it maintains.	Inspected the data retention, destruction, and reuse policy to determine that the entity established written policies related to retention periods for the confidential information it maintained.	No exceptions noted.
		Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Chief Information Security Officer regarding authorized personnel to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
			Inspected the network, database and VPN administrator user listings to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The entity establishes written policies related to the disposal of the confidential information it maintains.	Inspected the data retention, destruction, and reuse policy to determine that the entity established written policies related to the disposal of the confidential information it maintained.	No exceptions noted.
		As confidential data meets the retention period, the data is destroyed or purged.	Inquired of the Chief Information Security Officer regarding retention periods to determine that as confidential data meets the retention period, the data is destroyed or purged.	No exceptions noted.
			Inspected the data retention, destruction, and reuse policy to determine that 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 supporting service ticket for a sample of requests to dispose of data, purge a system, or physically destroy a system, to determine that as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.
		The entity purges confidential data stored on backup tapes and backup drives.	Inquired of the Chief Information Security Officer regarding purging of confidential data to determine that the entity purged confidential data stored on backup tapes and backup drives.	No exceptions noted.
			Inspected the data retention, destruction, and reuse policy to determine that the entity purged confidential data stored on backup tapes and backup drives.	No exceptions noted.
			Inspected the data destruction certificates to determine that the entity purged confidential data stored on backup tapes and backup drives.	Testing of the control activity disclosed that no confidential data destruction tasks were contracted out during the review period that would have garnered a certificate of destruction.