A-LIGN

ICE Consulting, Inc.

Type 2 SOC 2

2023

ICE
TRUSTED IT PARTNER

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

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

January 1, 2023 to December 31, 2023

Table of Contents

SECTION 1

ASSERTION OF ICE CONSULTING, INC. MANAGEMENT

ASSERTION OF ICE CONSULTING, INC. MANAGEMENT

March 15, 2024

We have prepared the accompanying description of ICE Consulting, Inc.'s ('ICE Consulting' or 'the Company') Managed IT Services System titled "ICE Consulting, Inc.'s Description of Its Managed IT Services System throughout the period January 1, 2023 to December 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Managed IT Services System that may be useful when assessing the risks arising from interactions with ICE Consulting's system, particularly information about system controls that ICE Consulting has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

ICE Consulting uses Amazon Web Services, Inc. ('AWS') to provide cloud hosting services and ConnectWise, LLC ('ConnectWise') to provide software as a service (SaaS) 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 ICE Consulting, to achieve ICE Consulting's service commitments and system requirements based on the applicable trust services criteria. The description presents ICE Consulting's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ICE Consulting's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents ICE Consulting's Managed IT Services System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that ICE Consulting's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of ICE Consulting's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that ICE Consulting's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ICE Consulting's controls operated effectively throughout that period.

Fred Care

Fred Care
Director of Operations
ICE Consulting, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ICE Consulting, Inc.

Scope

We have examined ICE Consulting's accompanying description of its Managed IT Services System titled "ICE Consulting, Inc.'s Description of Its Managed IT Services System throughout the period January 1, 2023 to December 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that ICE Consulting's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

ICE Consulting uses AWS to provide cloud hosting services and ConnectWise to provide software as a service (SaaS) services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ICE Consulting, to achieve ICE Consulting's service commitments and system requirements based on the applicable trust services criteria. The description presents ICE Consulting's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ICE Consulting's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ICE Consulting, to achieve ICE Consulting's service commitments and system requirements based on the applicable trust services criteria. The description presents ICE Consulting's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ICE Consulting's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects,

a. the description presents ICE Consulting's Managed IT Services System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that ICE Consulting's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of ICE Consulting's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that ICE Consulting's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ICE Consulting's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of ICE Consulting, user entities of ICE Consulting's Managed IT Services System during some or all of the period January 1, 2023 to December 31, 2023, business partners of ICE Consulting subject to risks arising from interactions with the Managed IT Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
March 15, 2024

SECTION 3

ICE CONSULTING, INC.'S DESCRIPTION OF ITS MANAGED IT SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2023 TO DECEMBER 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Founded in 1996, ICE Consulting offers a comprehensive range of managed IT services to small to medium-sized companies in a range of industries. ICE Consulting provides end-to-end, vendor-independent IT services, and offer specialized services in biotech and life sciences, as well as cloud services. ICE Consulting functions as standalone IT department, handling all aspects of IT for clients, or can provide IT consulting services.

Description of Services Provided

The services provided by ICE Consulting can be categorized into the following four groups:

1. IT Strategic services
    - Provide IT Director services
    - Design IT Infrastructure On-Premise and Cloud
    - Implement processes and procedures based on IT best practices
    - Meet compliance and Information Security requirements
    - Handle office build-out, migration and expansions

2. IT Technical services
    - Firewall, Switching and Routing
    - Linux, Windows and Mac servers and systems
    - Cybersecurity
    - Virtualization and Storage
    - Backup and Disaster Recovery
    - Wireless solutions
    - Single sign on (SSO) and Multifactor Authentication
    - Mobile Device Management (MDM)
    - Cloud services management
    - Onboarding and offboarding employees and contractors
    - Printing and phone services

3. IT Support services
    - Onsite technical services
    - Helpdesk-live tech support 24x7x365 including holidays
    - Proactive weekly Preventive Maintenance:
        - Network Security
        - Network Infrastructure
        - Systems Infrastructure
        - Endpoints (Desktops, Laptops and Mobile devices)
    - NOC (Network Operation Center) 24x7x365
    - SOC (Security Operations Center) 24x7x365
    - Provide IT training to users

4. IT Administrative services
    - Regular IT meeting
    - Project Management
    - Ticket Management
    - Client Satisfaction Reporting
    - Weekly and Monthly IT Reporting

- Key Performance Index (KPI) Reporting
- Hardware and Software procurement
- Asset Management
- Vendor management
- Cabling services
- IT Room, Cooling, HVAC
- IT Documentation

Principal Service Commitments and System Requirements

ICE principal service commitments are based on the SLA and the IT inventory under managed services. ICE Consulting offers four different types of SLAs namely Platinum, Gold, Silver and Bronze. Each of the SLA's type have different response and uptime commitments.

Components of the System

Infrastructure

Primary infrastructure used to provide ICE Consulting's Managed IT Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Edge Switch	Brocade 6430	Directs traffic to Firewall and VPN
Firewall	Fortigate 100E	Filters traffic into and out of the private network supporting the corporate services
VPN	PSA 3000	Provides VPN services for remote workers to access internal resources
Core Switches	Ruckus/Brocade ICS6610	Connects servers and storage to internal network
Access Switches	Ruckus/Brocade ICS6610	Connects devices on the internal network
Server	Hp ProLiant DL360 Gen 10	ESxi (Virtualization)
Server	Hp ProLiant DL360 Gen 10	ESxi (Virtualization)
Server	Super Micro- Super Server	Veeam Backup
Server	PowerEdge R210	Physical Domain Controller
Storage	NetApp FAS2554 (Two Units in HA)	Storage for Servers (Fileserver, DC's, Application Servers)
Tape Library	Neo Series-FlexStor II LTO-7	Backup of Servers using Veeam Backup
UPS	APC RM3000	Uninterrupted Power Supply to ICE Consulting Datacenter Hardware

Software

Primary software used to provide ICE Consulting's Managed IT Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
VMware ESXi	7.0.2.17367351	Host Virtual Machines/Servers
vCenter 6	7.0.3.00600	Management of ESXi Hosts
Veeam Backup 10	Windows Server 2016	Backup of Servers (Fileserver, DC's, Application Servers)
ConnectWise 2022.1	Windows Server 2019	Client Support Ticketing System, Project Management
RDM	Windows Server 2012 R2	Remote Access Management
MS SQL2019	Windows Server 2019	Database of ConnectWise Server
Carbon Black (EDR)	Hosted On Cloud	Antivirus Solution- Endpoint detection and response
Workspace One	VMware Cloud	To centrally control and manage end users' mobile devices, Desktops and Laptops
BrightGauge	Hosted On Cloud	Real-time dashboard of Clients Tickets and reporting
Zoom	Hosted on Cloud	Cloud platform for video, voice, content sharing, and chat runs across mobile devices, desktops, telephones, and room systems
Bomgar (Beyond Trust)	Hosted On Cloud	Secure Remote Support
CheckMK	Ubuntu Linux (64-bit)	Monitoring of entire IT infrastructure (servers, applications, networks, storage, databases)
Slack	Hosted On Cloud	to bring together internal communication and collaboration into one place
Code42	Hosted On Cloud	Endpoint Backups on Cloud (Laptops, Desktops)
OKTA	Hosted On Cloud	Single Sign On and Multifactor Authentication to Apps and Services
AWS - Cloud Computing Services	On AWS Cloud	Ice Consulting have hosted ConnectWise and domain controller on AWS
Microsoft 365	Hosted on Cloud	MS Office Apps (Word, Excel, PowerPoint, Outlook, Visio) and e-mail Services
ProofPoint	Hosted on Cloud	E-mail Spam Filtering, inbound e-mail security, e-mail encryption
Paycor	Hosted on Cloud	HR / Payroll Management
QuickBooks	Hosted on Cloud	Financial management system

People

ICE Consulting has a staff of approximately 70 employees organized in the following functional areas:

- Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources.
- Operations. Staff that administers the scheduling and administration of Customer Success Managers. They provide the direct day-to-day services, such as:
    - Customer Success Managers take phone calls directly from Clients to resolve issues and requests. These requests are entered into the ConnectWise Ticketing Systems and initiate the life cycle of an issue or requests.
    - They also manage dispensing work from the ConnectWise to the engineers.
    - Quality assurance (or utilization review) employees use reports generated by the ConnectWise.
- IT Help desk, IT network engineers, IT system administration, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom:
    - The help desk group provides technical assistance to the ICE Consulting users.
    - The infrastructure, networking, and systems administration staff typically supports ICE Consulting's IT infrastructure, which is used by the Users A systems administrator will deploy the releases of the ConnectWise and other software into the production environment.
    - The information security staff supports the ICE Consulting infrastructure indirectly by monitoring internal and external security threats and maintaining current antivirus software.
    - The information security staff maintains the inventory of IT assets.

Data

Ice Consulting securely keeps client's data on fileserver, Confluence Server, ConnectWise ticketing system and RDM. These all are inhouse servers and applications secured using Active Directory and multifactor authentication with strong password policy. No external user has access to servers and services and ICE Consulting sets up strong security and permissions on the fileserver. ICE Consulting requires approvals from management to grant permissions to internal users. Data stored is fully encrypted. All passwords stored in the data sources-RDM are encrypted using a strong encryption algorithm, to the extent that if a user attempts to access the data directly in the database, it will be considered unreadable. Advanced Encryption Standard (AES) algorithm to protect sensitive data in the RDM database. ICE Consulting sets up SSL certificate and secured information on confluence and ConnectWise servers and implemented MFA for authentication.

Processes, Policies and Procedures

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

<u>Physical Security</u>

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

Logical Access

ICE uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, ICE Consulting implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

Employees sign on to the ICE Consulting network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the ICE Consulting network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview.

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

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

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

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

The HR system generates a list of terminated employees as needed basis. This report is used by the IT help desk to delete employee access. On a quarterly basis, HR runs a list of active employees. The IT help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

On an annual basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the IT help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the ISO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

Ice Consulting takes backups of all servers and services which includes Fileserver, DC's, Databases, Application servers, ConnectWise Application, and database server, RDM, ShoreTel voice System, Desktop VDI's, Utility Servers, Linux servers (CheckMK Monitoring, SMTP relay) on daily (Incremental), weekly (Full), Monthly (Full) on on-Site Disk Storage and from there backups are synched to offsite AWS S3 Storage.

Backup jobs are configured to notify on Success, Warning, and failed job events. In case a backup job is failed or in warning state a troubleshooting procedure is in place and the job is run until its successful completion.

Computer Operations - Availability

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.

ICE monitors the capacity utilization of physical and computing infrastructure to ensure that service delivery matches service level agreements. ICE Consulting evaluates the need for additional infrastructure capacity in response to growth in capacity demand. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

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

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

Change Control

ICE maintains documented baseline requirements for the configuration of IT systems and tools. Any system upgrades or patches must be authorized by management prior to implementation. Access to implement upgrades and patches to systems is restricted to authorized IT personnel.

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

Data Communications

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

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

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

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

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

Please refer to the 'Subservice Organizations' section below for further details on the specific change management controls implemented by ConnectWise.

Boundaries of the System

The scope of this report includes the Managed IT Services System performed in the Milpitas, California facilities.

This report does not include the cloud hosting services provided by AWS at multiple facilities or the SaaS services provided by ConnectWise at multiple facilities.

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

Control Environment

Integrity and Ethical Values

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

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.

- Policies and procedures require employees 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

ICE Consulting's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for positions 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

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

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

- Management is briefed on regulatory and industry changes affecting the services provided at least annually.
- 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

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

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

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated at least annually.

Human Resource Policies and Practices

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

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

- New employees are required to sign 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

ICE Consulting 's risk assessment process identifies and manages risks that could potentially affect ICE Consulting's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ICE Consulting 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 ICE, 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

ICE 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. ICE Consulting 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

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

Information and Communications Systems

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

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate ICE Consulting personnel via e-mail messages.

Specific information systems used to support ICE Consulting's Managed IT Services System are described in the Description of Services section above.

Monitoring Controls

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

On-Going Monitoring

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

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

Reporting Deficiencies

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. 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 criteria are applicable to the ICE Consulting Managed IT Services System, with the exception of Software Development Services. ICE utilizes only Off-The-Shelf applications and hosted services to operate its business.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities or the SaaS services provided by ConnectWise at multiple facilities.

Subservice Description of Services

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

Complementary Subservice Organization Controls

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

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

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

Subservice Organization - ConnectWise		
Category	**Criteria**	**Control**
Common Criteria/Security	CC8.1	A ticketing system is used by IT and customer support teams to monitor and track infrastructure and application issues and events from identification to resolution.
		Changes to the application are tested and approved by QA prior to deployment into production.
		Application changes are reviewed by a technical peer for appropriateness of code change, secure coding techniques, and test plans prior to approval for migration to production.
		A code versioning platform is used to track changes to scripts used to automate the deployment of servers based on application function.
		An e-mail alert to the development distribution group is generated when a new build is promoted to production.

ICE Consulting 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 service level agreements. In addition, ICE Consulting performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

Ice Consulting's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to ICE Consulting's services to be solely achieved by ICE Consulting control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ICE Consulting's.

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

1. User entities are responsible for understanding and complying with their contractual obligations to ICE Consulting.
2. User entities are responsible for ensuring the supervision, management, and control of the use of ICE Consulting services by their personnel.
3. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Ice Consulting services.
4. User entities are responsible for immediately notifying ICE Consulting of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

5. User entities are responsible for notifying ICE Consulting of changes made to technical or administrative contact information.
6. User entities are responsible for developing and maintaining their own change management policies and procedures.
7. User entities are responsible for ensuring that all changes follow their defined system development lifecycle.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

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

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee manual handbook, code of conduct, and the entity's intranet shared drive to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct for a sample new hire to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Upon hire, personnel are required to sign a non-disclosure agreement.	Inspected the signed employee confidentiality agreement for a sample of new hires to determine that upon hire, personnel were required to sign a non-disclosure agreement.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to complete a background check.	Inspected the background check policies and procedures and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and the code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which include probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the escalation policies and procedures and employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement requires that third-parties have a code of conduct and employee handbook in place.	Inspected the third-party agreement template to determine that the entity's third-party agreement required that third-parties have a code of conduct and employee handbook in place.	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement required that third-parties have a code of conduct and employee handbook in place.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the documented executive job description including revision date for a sample of executive job roles to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the documented executive job description including revision date for a sample of roles to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the completed performance review form for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management maintains independence from those that operate the key controls implemented 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 implemented within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually.	Inspected the evaluation form for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the management meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample job role and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for an example job role to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct for a sample new hire to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, internal controls matrix, a sample job description to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the third-party risk and security management policy to determine that a vendor risk assessment was required on an annual basis.	No exceptions noted.
			Inspected the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	Inspected the interview evaluation for an example new hire to determine that the entity evaluated the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inspected the job description for an example job role and the interview evaluation for an example new hire to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the recruiting policies and procedures to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the continuing professional education (CPE) training tracker to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
			Inspected the training completion certificates for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management uses an outside vendor to assist with its continued training of employees.	Inspected the information security awareness training materials to determine that executive management created a training program for its employees.	No exceptions noted.
			Inspected the third-party agreement to determine that executive management used an outside vendor to assist with its continued training of employees.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management tracks and monitors compliance with continued professional education training requirements.	Inspected the CPE training tracker to determine that executive management tracked and monitored compliance with continued professional education training requirements.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it relates to their job role and responsibilities.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the training assessment to determine that the entity assessed the training needs on an annual basis.	No exceptions noted.
		As part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trains its personnel.	Inspected the training materials to determine that as part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trained its personnel.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the background check policies and procedures and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check prior to employment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample job role and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the signed employee handbook and the code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and the code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.
		Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary.	Inspected the compliance review meeting minutes to determine that executive management reviewed the responsibilities assigned to operational personnel annually updates were made, as necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies which included probation, suspension and termination were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	Inspected the information security policies and procedures, job description for a sample of job roles and the entity's shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the entity’s data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access.	Inspected the IPS configurations, encryption methods and configurations and VPN authentication configurations to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the data retention and disposal policy to determine that data was retained for only as long as required to perform the required system functionality, service, or use.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample job role and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's intranet.	Inspected the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the entity's intranet.	No exceptions noted.
		Upon hire, employees are required to complete information security awareness training.	Inspected the information security awareness training tracking tool for a sample of new hires to determine that upon hire, employees were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to complete information security awareness training on an annual basis.	Inspected the information security awareness training tracking tool for a sample of current employees to determine that current employees were required to complete information security awareness training on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct for a sample new hire to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the executive committee agenda meeting minutes to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the escalation policies and procedures and employee handbook to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet.	Inspected the incident management policies and procedures and the entity's intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's intranet.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's shared drive.	Inspected the entity's shared drive to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's shared drive.	No exceptions noted.
		Management tracks and monitors compliance with information security awareness training requirements.	Inspected the security awareness training dashboard to determine that management tracked and monitored compliance with information security awareness training requirements.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement for a sample third-party to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the third-party agreement for a sample third-party to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties.	Inspected the third-party agreement for a sample third-party to determine that the entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties.	No exceptions noted.
		The entity's contractor agreement outlines and communicates the terms, conditions, and responsibilities of external users.	Inspected the contractor agreement to determine that the entity's contractor agreement outlined and communicated the terms, conditions, and responsibilities of external users.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the customer agreement template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the agreement for a sample customer to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via updated agreements.	Inspected the e-mail communicating updated commitments via an updated agreement to an example client to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users, and customers via updated agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.	Inspected the customer SLAs to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and shared with external parties.	No exceptions noted.

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 handbook and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant, and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were specific, measurable, attainable, relevant, and time-bound (SMART).	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the IT risk management policy to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the Network and Security Engineering Audit Manager and IT Director job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	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 handbook the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the management meeting minutes to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the IT risk management policy to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	Inspected the IT risk management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	Inspected the IT risk management policy to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	No exceptions noted.
		Identified risks are rated using a risk evaluation process.	Inspected the IT risk management policy to determine that identified risks were rated using a risk evaluation process.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the IT risk management policy to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
			Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the IT risk management policy to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
			Inspected the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	Inspected the IT risk management policy to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.
			Inspected the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.

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 business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the IT risk management policy to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the IT risk management policy to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the IT risk management policy to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the management meeting minutes to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Logical access reviews are performed on an annual basis.	Inspected the completed user access review to determine that logical access reviews were performed on an annual basis.	No exceptions noted.
		Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results and information security policy to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerability scans are performed quarterly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan results for a sample of quarters to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		External penetration testing is done annually to identify and exploit vulnerabilities identified within the environment.	Inspected the information security policy to determine that external penetration testing was done annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-parties environment.	Inspected the third-party risk and security management policy to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-parties environment.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.	Inspected the IT risk management policy, completed risk and compliance assessments to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.	Inspected the IT risk management policy, completed risk and compliance assessments to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were documented, investigated, and addressed.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the entity's internal helpdesk ticketing system to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	Inspected the IT risk management policy completed risk assessment and internal control matrix to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Inspected the IT risk management policy, completed risk assessment, and completed compliance assessment to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the IT risk management policy to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Business continuity plans are developed and updated on an annual basis.	Inspected the business continuity plan to determine that business continuity plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity plans are tested on an annual basis.	Inspected the completed business continuity test results to determine that the business continuity 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.	Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet.	Inspected the information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's intranet.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what was required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet.	Inspected the information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's intranet.	No exceptions noted.
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the employee handbook and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the employee handbook and information security policies and procedures and internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample job role and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network (AWS and Active Directory)			
		Network user access is restricted via role-based security privileges defined within the access control systems.	Inspected the network user listings and access rights to determine that network user access was restricted via role-based security privileges defined within the access control systems.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Chief Finance Officer • Business Manager	Inquired of the Information Security Officer regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Chief Finance Officer • Business Manager	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network administrator listings and access rights to determine that network administrative access was restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Chief Finance Officer • Business Manager	No exceptions noted.
		Networks are configured to enforce password requirements that include: AD: • Password history • Password expiration • Password length • Complexity AWS: • Password length • Complexity	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
		Network users are authenticated via individually-assigned user accounts and passwords.	Observed the Information Security Officer login to the network to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Active Directory account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging settings are in place that include: AD: • Account logon events • Account management • Directory Service Access • Logon events AWS: • Management events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: AD: • Account logon events • Account management • Directory Service Access • Logon events AWS: • Management events	No exceptions noted.
		Network audit logs are maintained and reviewed if-needed.	Inquired of the Information Security Officer regarding network audit logs to determine that network audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed if-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System (Windows, Linux)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Windows operating system administrative access is restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Business Manager	Inquired of Information Security Officer regarding administrative access to determine that windows operating system administrative access was restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Business Manager	No exceptions noted.
			Inspected the operating system administrator listing and access rights to determine that windows operating system administrative access was restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Business Manager	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**
		Linux operating system administrative access is restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Compliance Consultant • Business Manager • Network Team Engineer • Network Engineer	Inquired of Information Security Officer regarding administrative access to determine that Linux operating system administrative access was restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Compliance Consultant • Business Manager • Network Team Engineer • Network Engineer	No exceptions noted.
			Inspected the operating system administrator listing and access rights to determine that Linux operating system administrative access was restricted to user accounts accessible by the following personnel: • Systems Team Manager • Systems Engineer • Chief Executive Officer • Compliance Consultant • Business Manager • Network Team Engineer • Network Engineer	No exceptions noted.
		Windows operating systems are configured to use Active Directory for single sign-on (SSO).	Inspected the operating system password settings to determine that operating systems were configured to use Active Directory for SSO.	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**
		Linux operating systems are configured to authenticate users via secure shell (SSH) keys.	Observed a user access a Linux server to determine that Linux operating systems were configured to authenticate users via SSH keys.	No exceptions noted.
			Inspected the Linux operating system authentication configurations to determine that Linux operating systems were configured to authenticate users via SSH keys.	No exceptions noted.
		Windows operating system users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the operating system to determine that windows operating system users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Windows operating system audit logging settings are in place that include: • Account logon events • Logon events	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that windows operating system audit logging configurations were in place that included: • Account logon events • Logon events	No exceptions noted.
		Linux operating system audit logging settings are in place that include: • Logon events • Local events • Privileged access	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that Linux operating system audit logging settings were in place that include: • Logon events • Local events • Privileged access	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system audit logs are maintained and reviewed if-needed.	Inquired of Information Security Officer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed if-needed. Inspected an example operating system activity audit log extract to determine that operating system audit logs were maintained and reviewed if-needed.	No exceptions noted. No exceptions noted.
	Database (SQL)			
		Database user access is restricted via role-based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by the following personnel: • Chief Executive Officer • Business Manager • Systems Engineer • Database Administrator	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system. Inquired of Information Security Officer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by the following personnel: • Chief Executive Officer • Business Manager • Systems Engineer • Database Administrator	No exceptions noted. 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 the following personnel: • Chief Executive Officer • Business Manager • Systems Engineer • Database Administrator	No exceptions noted.
		SQL databases are configured to use mixed mode authentication.	Inspected the database password settings to determine that the MySQL database was configured to use mixed mode authentication.	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Database audit logging settings are in place that include failed logins.	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Failed logins	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logs are maintained and reviewed if-needed.	Inquired of Information Security Officer regarding database audit logs to determine that the database audit logs were maintained and reviewed if-needed. Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed if-needed.	No exceptions noted. No exceptions noted.
	Application (ConnectWise)			
		Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by the following personnel: • Chief Executive Officer • Compliance Consultant • Business Manager • Network Team Engineer • Network Engineer • Systems Team Manager • Systems Engineer	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system. Inquired of Information Security Officer regarding administrative access to determine that application administrative access was restricted to user accounts accessible by the following personnel: • Chief Executive Officer • Compliance Consultant • Business Manager • Network Team Engineer • Network Engineer • Systems Team Manager • Systems Engineer	No exceptions noted. No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel: • Chief Executive Officer • Compliance Consultant • Business Manager • Network Team Engineer • Network Engineer • Systems Team Manager • Systems Engineer	No exceptions noted.
		The application is configured to use Active Directory credentials for authentication.	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
		Application users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the application to determine that application users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit logging settings are in place that include: • Account logon events • Logon events	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Logon events	No exceptions noted.
		Application audit logs are maintained and reviewed if-needed.	Inquired of Information Security Officer regarding application audit logs to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
	Remote Access			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • Compliance Consultant • Network Team Engineer • Network Engineer	Inquired of the Information Security Officer regarding VPN administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel: • Compliance Consultant • Network Team Engineer • Network Engineer	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel: • Compliance Consultant • Network Team Engineer • Network Engineer	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Observed a user authenticate to the VPN access to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
			Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the interfaces configurations to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IPS.	Inspected the IPS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IPS.	No exceptions noted.
		A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Stored passwords are encrypted.	Inspected the encryption configurations for data at rest to determine that stored passwords were encrypted.	No exceptions noted.
		Critical data is stored in encrypted format using Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA).	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES, and RSA.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Encryption keys are protected during generation, storage, use, and destruction.	Inspected the data encryption policy to determine that encryption keys were protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed on an annual basis.	Inspected the information security policy to determine that logical access reviews were performed on an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the information security policy to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the information security policy to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on an annual basis.	Inspected the completed user access review to determine that logical access reviews were performed on an annual basis.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		An analysis of incompatible operational duties is performed on an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the compliance review meeting minuets to determine that an analysis of incompatible operational duties was performed on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the information Security Officer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database, and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed on an annual basis.	Inspected the completed user access review to determine that logical access reviews were performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Operating System			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database (SQL)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Application (Connectwise)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

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 policies and procedures to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
		Physical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring policy, badge access listings and user access request e-mail for a sample of new hires to determine that physical access was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		A badge access system controls access to and within the office facility.	Inspected the badge access listing to determine that a badge access system controlled access to and within the 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.
		The badge access system logs successful access attempts. The logs can be pulled for review if necessary.	Inspected badge access log for an example day to determine that the badge access system logged successful and failed access attempts and 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**
		Privileged access to the badge access system was restricted to persons holding the following positions: • Client Success Manager • CEO	Inquired of the Information Security Officer regarding privileged access to determine that privileged access to the badge access system was restricted to persons holding the following positions: • Client Success Manager • CEO	No exceptions noted.
			Inspected the badge access administrator listing to determine that badge access system was restricted to persons holding the following positions: • Client Success Manager • CEO	No exceptions noted.
		Access to the server room / data center is restricted to individuals with physical keys.	Inquired of the Information Security Officer regarding access to the server room to determine that access to the server room/data center was restricted to individuals with physical keys.	No exceptions noted.
			Inspected the key log to determine that access to the server room / data center was restricted to individuals with physical keys.	No exceptions noted.
		A video surveillance system is in place with footage retained for 60 days.	Inspected the video surveillance system configurations and oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for 60 days.	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**
		Visitors to the facility and server room are escorted by an authorized employee.	Inspected the physical security policy to determine that visitors to the facility and server room were escorted by an authorized employee.	No exceptions noted.
		Visitors to the facility and server room are required to sign a visitor log prior upon arrival.	Inspected a visitor log for an example day to determine that visitors to the facility and server room were required to sign a visitor log prior upon arrival.	No exceptions noted.
		Physical access to systems is revoked as a component of the termination process.	Inspected the termination checklist and policy, badge access user listing, user termination e-mails, and user badge access revocation for a sample of terminated employees to determine that physical access to systems was revoked as a component of the termination process.	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity purges data per a defined schedule.	Inspected the data retention and disposal policy to determine that the entity purged data per a defined schedule.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Information Security Officer regarding data disposal and destruction to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the data retention and disposal policies to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the supporting ticket for a sample of data disposals to determine that data that was no longer required for business purposes was rendered unreadable.	Testing of the control activity disclosed that there were no data disposals during the review period.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the removable media policies and procedures to determine that policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN, SSL, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Observed a user authenticate to the VPN access to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
			Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Information Security Officer regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram 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				
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 firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An intrusion prevention system (IPS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected an example IPS log extract and alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on-access.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on-access.	No exceptions noted.
		Critical data is stored in encrypted format using AES, and RSA.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES, and RSA.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to authorized personnel.	Inquired of the Information Security Officer regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Backup media is replicated off-site on a monthly basis.	Inspected the backup replication schedule configurations to determine that backup media was rotated off-site by a third-party vendor monthly.	No exceptions noted.
		The ability to access backup tapes is restricted to authorized personnel.	Inquired of the Information Security Officer regarding access to stored data regarding the ability to recall backed up data to determine that the ability to access backup tapes was restricted to authorized personnel.	No exceptions noted.
			Inspected the server room key log to determine that the ability to access backup tapes was restricted to authorized personnel.	No exceptions noted.
		The entity secures its environment using a multi-layered defense approach that includes firewalls, an IPS antivirus software and a DMZ.	Inspected the network diagram, IPS configurations, firewall rule sets, antivirus settings and DMZ settings to determine that the entity secured its environment using a multi-layered defense approach that included firewalls, an IPS antivirus software and a DMZ.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN, SSL, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

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 firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected an example IPS log extract and alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		Critical data is stored in encrypted format using AES, and RSA.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES, and RSA.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
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 entity restricts users access to only approved webpages.	Inspected the blocking message on a restricted website to determine that the entity restricted users' access to only approved webpages.	No exceptions noted.
		Access to implement upgrades and patches is restricted to authorized IT personnel.	Inquired of the Information Security Officer regarding access to upgrades and patches to determine that access to implement upgrades and patches was restricted to authorized IT 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 list of users with access to deploy upgrades and patches into the production environment to determine that access to implement upgrades and patches was restricted to authorized IT personnel.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on-access.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on-access.	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, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example log extract from the IPS and an example IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected an example IPS log extract and alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

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**
		Vulnerability scans are performed quarterly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan results for a sample of quarters to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example log extract from the IPS and an example IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected an example IPS log extract and alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on-access.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on-access.	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**
	Physical			
		CCTV cameras monitor physical access to the entity's facilities and visitor access to the facility and server room. The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected the video surveillance configurations to determine that CCTV cameras monitor physical access to the entity's facilities and visitor access to the facility and server room. Inspected the badge access log for an example day to determine that the badge access system logged successful and failed access attempts and logs could be pulled for review if necessary.	No exceptions noted. No exceptions noted.
	Network (AWS and Active Directory)			
		Active Directory account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging settings are in place that include: AD: • Account logon events • Account management • Directory Service Access • Logon events AWS: • Management events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: AD: • Account logon events • Account management • Directory Service Access • Logon events AWS: • Management events	No exceptions noted.
		Network audit logs are maintained and reviewed if-needed.	Inquired of the Information Security Officer regarding network audit logs to determine that network audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed if-needed.	No exceptions noted.
	Operating System (Windows and Linux)			
		Windows operating system audit logging settings are in place that include: • Account logon events • Logon events	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that windows operating system audit logging configurations were in place that included: • Account logon events • Logon events	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**
		Linux operating system audit logging settings are in place that include: • Logon events • Local events • Privileged access	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that Linux operating system audit logging settings were in place that include: • Logon events • Local events • Privileged access	No exceptions noted.
		Operating system audit logs are maintained and reviewed if-needed.	Inquired of Information Security Officer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected an example operating system activity audit log extract to determine that operating system audit logs were maintained and reviewed if-needed.	No exceptions noted.
	Database (SQL)			
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging settings are in place that include: • Failed logins	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Failed logins	No exceptions noted.
		Database audit logs are maintained and reviewed if-needed.	Inquired of Information Security Officer regarding database audit logs to determine the database audit logs were maintained and reviewed if-needed.	No exceptions noted.
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed if-needed.	No exceptions noted.
	Application (ConnectWise)			
		Application audit logging settings are in place that include: • Account logon events • Logon events	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Logon events	No exceptions noted.
		Application audit logs are maintained and reviewed if-needed.	Inquired of Information Security Officer regarding application audit logs to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed if-needed.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed annually for effectiveness.	Inspected the revision history of the incident response policy to determine that the incident response and escalation procedures were reviewed annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that resolution of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no incident took place within the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for an example incident to determine that incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no incident took place within the review period.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response plan to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no incidents occurred within the review period.
		Identified incidents are reviewed, monitored, and investigated by an incident response team.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that identified incidents are reviewed, monitored, and investigated by an incident response team.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that identified incidents are reviewed, monitored, and investigated by an incident response team.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that identified incidents are reviewed, monitored, and investigated by an incident response team.	Testing of the control activity disclosed that no incident took place within the review period.
		Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	Testing of the control activity disclosed that no incident took place within the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no incident took place within the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that the actions taken to address identified security incidents are documented and communicated to affected parties.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the actions taken to address identified security incidents are documented and communicated to affected parties.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that the actions taken to address identified security incidents are documented and communicated to affected parties.	Testing of the control activity disclosed that no incident took place within the review period.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that resolution of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no incident took place within the review period.
		Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy.	Testing of the control activity disclosed that no incident took place within the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response plan to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no incidents occurred within the review period.
		The incident response and escalation procedures are reviewed annually for effectiveness.	Inspected the revision history of the incident response policy to determine that the incident response and escalation procedures were reviewed annually for effectiveness.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the information, software, and system backup policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response plan to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for an example incident to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no incidents occurred within the review period.
		After critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned.	Inquired of the Information Security Officer regarding the documented incident tickets to determine that after critical incidents were investigated and addressed, lessons learned were documented and analyzed, and incident response plans and recovery procedures were updated based on the lessons learned.	
			Inspected the incident response policies and procedures to determine that after critical incidents were investigated and addressed, lessons learned were documented and analyzed, and incident response plans and recovery procedures were updated based on the lessons learned.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for an example incident to determine that after critical incidents were investigated and addressed, lessons learned were documented and analyzed, and incident response plans and recovery procedures were updated based on the lessons learned.	Testing of the control activity disclosed that no incidents occurred within the review period.
		Business continuity plans are developed and updated on an annual basis.	Inspected the business continuity plans to determine that business continuity plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity plans are tested on an annual basis.	Inspected the completed business continuity plan test results to determine that the business continuity 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 change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the system change e-mail notifications to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		Access to implement upgrades and patches is restricted to authorized IT personnel.	Inquired of the Information Security Officer regarding the patch authorization access to determine that access to implement upgrades and patches 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**
			Inspected the list of users with access to deploy upgrades and patches into the production environment to determine that access to implement upgrades and patches was restricted to authorized IT personnel.	No exceptions noted.
		System upgrades and patches are authorized and approved by management prior to implementation.	Inspected the supporting change documentation for a sample application update, infrastructure change, and operating system change to determine that system upgrades and patches were authorized and approved by management prior to implementation.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software settings to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.	Not Applicable.	Not Applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the IT risk management policy to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	Inspected the IT risk management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the IT risk management policy to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the customer agreement for a sample of customers to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-parties environment.	Inspected the completed third-party attestation report 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-parties environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures to determine that a vendor risk assessment was required on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.