XBRL US, Inc.
Type 2 SOC 2
2018

REPORT ON XBRL US, 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 Service Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

August 1, 2017 through October 31, 2018

Table of Contents

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT 1

SECTION 2 MANAGEMENT OF XBRL US, INC.'S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2017 THROUGH OCTOBER 31, 2018 4

SECTION 3 DESCRIPTION OF XBRL US, INC.'S SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2017 THROUGH OCTOBER 31, 2018 7

- OVERVIEW OF OPERATIONS 8
  - Company Background 8
  - Description of Services Provided 8
- CONTROL ENVIRONMENT 14
  - Integrity and Ethical Values 14
  - Commitment to Competence 14
  - Management's Philosophy and Operating Style 14
  - Organizational Structure and Assignment of Authority and Responsibility 15
  - Human Resources Policies and Practices 15
- RISK ASSESSMENT 15
- TRUST SERVICES PRINCIPLES AND CRITERIA 16
- MONITORING 16
- INFORMATION AND COMMUNICATION SYSTEMS 17
- COMPLEMENTARY USER ENTITY CONTROLS 17

SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR 18

- GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 19
  - COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES 20

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT XBRL US, INC. RELEVANT TO SECURITY

To XBRL US, Inc.:

We have examined the attached description titled "Description of XBRL US, Inc.'s Tools for SEC Filers System Throughout the Period August 1, 2017 through October 31, 2018" (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the Security principle set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period August 1, 2017 through October 31, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of XBRL US, Inc.'s ('XBRL US' or 'the Company') controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

XBRL US uses Amazon Web Services ("subservice organization") for data center hosting services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents XBRL US's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

XBRL US has provided the attached assertion titled "Management of XBRL US, Inc.'s Assertion Regarding Its Tools for SEC Filers System Throughout the Period August 1, 2017 through October 31, 2018," which is based on the criteria identified in management's assertion. XBRL US is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in XBRL US's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination 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, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period August 1, 2017 through October 31, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in XBRL US's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period August 1, 2017 through October 31, 2018.
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period August 1, 2017 through October 31, 2018, and user entities applied the complementary user-entity controls contemplated in the design of XBRL US's controls throughout the period August 1, 2017 through October 31, 2018 and the subservice organization applied, throughout the period August 1, 2017 through October 31, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.
c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, and together with the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period August 1, 2017 through October 31, 2018.

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Information Provided by the Service Auditor".

This report and the description of tests of controls and results thereof are intended solely for the information and use of XBRL US; user entities of XBRL US's Tools for SEC Filers System during some or all throughout the period August 1, 2017 through October 31, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, 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, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria 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

January 23, 2019
Tampa, Florida

SECTION 2

MANAGEMENT OF XBRL US, INC.’S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2017 THROUGH OCTOBER 31, 2018

Management of XBRL US, Inc.’s Assertion Regarding Its System Throughout the Period August 1, 2017 through October 31, 2018

January 23, 2019

We have prepared the attached description titled "Description of XBRL US, Inc.’s Tools for SEC Filers System Throughout the Period August 1, 2017 through October 31, 2018" (the description), based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization’s system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Tools for SEC Filers System, particularly system controls intended to meet the criteria for the Security principle set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Tools for SEC Filers System throughout the period August 1, 2017 through October 31, 2018, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided.

(2) The components of the system used to provide the services, which are the following:

- *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
- *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Processes*. The automated and manual procedures.
- *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities or other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization’s system.

(8) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.

(9) Other aspects of the service organization’s control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) Relevant details of changes to the service organization’s system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization’s system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Campbell Pryde
President and CEO
XBRL US, Inc.

SECTION 3

DESCRIPTION OF XBRL US, INC.'S SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2017 THROUGH OCTOBER 31, 2018

OVERVIEW OF OPERATIONS

Company Background

XBRL US, Inc. is an industry-driven non-profit standards organization incorporated in Delaware in 2007 as a 501c6. As a recognized jurisdiction of XBRL International, which maintains the specification for the data standard (based on XML), XBRL US is responsible for building and promoting the use of financial data standards in U.S. markets to improve the efficiency and quality of reporting. The members of XBRL US are accounting firms, data and analytics providers, filing agents, public companies, other not-for-profits, startup tool providers, and stakeholders in reporting domains including insurance, energy and corporate actions.

Description of Services Provided

In order to facilitate the creation of standardized data in submissions to the U.S. Securities and Exchange Commission ("the SEC") by public companies complying with SEC rule 33-9002 (https://www.sec.gov/rules/final/2009/33-9002.pdf) , XBRL US initially developed the Tools for SEC Filers System (re-branded as XBRL US Tools for SEC Filers in 2015) to provide a mechanism for SEC filers and other users of US GAAP to check that documents prepared in XBRL meet minimum quality standards related to the use of US GAAP and XBRL. The XBRL US Tools for SEC Filers System ('the System') provides approximately 10,000 automated edit rules that check for inconsistencies in US GAAP filings. The System does not test that a filing is XBRL valid or that it complies with the SEC filing manual. The service assumes the filings are XBRL valid (the system will reject invalid XBRL filings) and SEC valid. The system checks that tags used in the filing have appropriate values, that GAAP requirements have been met, and that tagged values are not inconsistent.

The rules used to check filings are updated at a minimum on a quarterly basis and from time to time to address timely issues. New rules are added based on errors seen in previous filings, new best practices, and problems identified by users trying to consume the XBRL data. The system securely processes a company's SEC filing in the System prior to SEC submission in order for company management to review the accuracy of their XBRL filing in a timely and accurate manner. To perform these rules manually would be extremely time consuming.

In order to check a filing, a user entity submits the XBRL documents to the System as a zip file. The zip file contains the XBRL exhibits the user intends to subsequently submit to the SEC. The zip file can be submitted to the System through one of the following means:

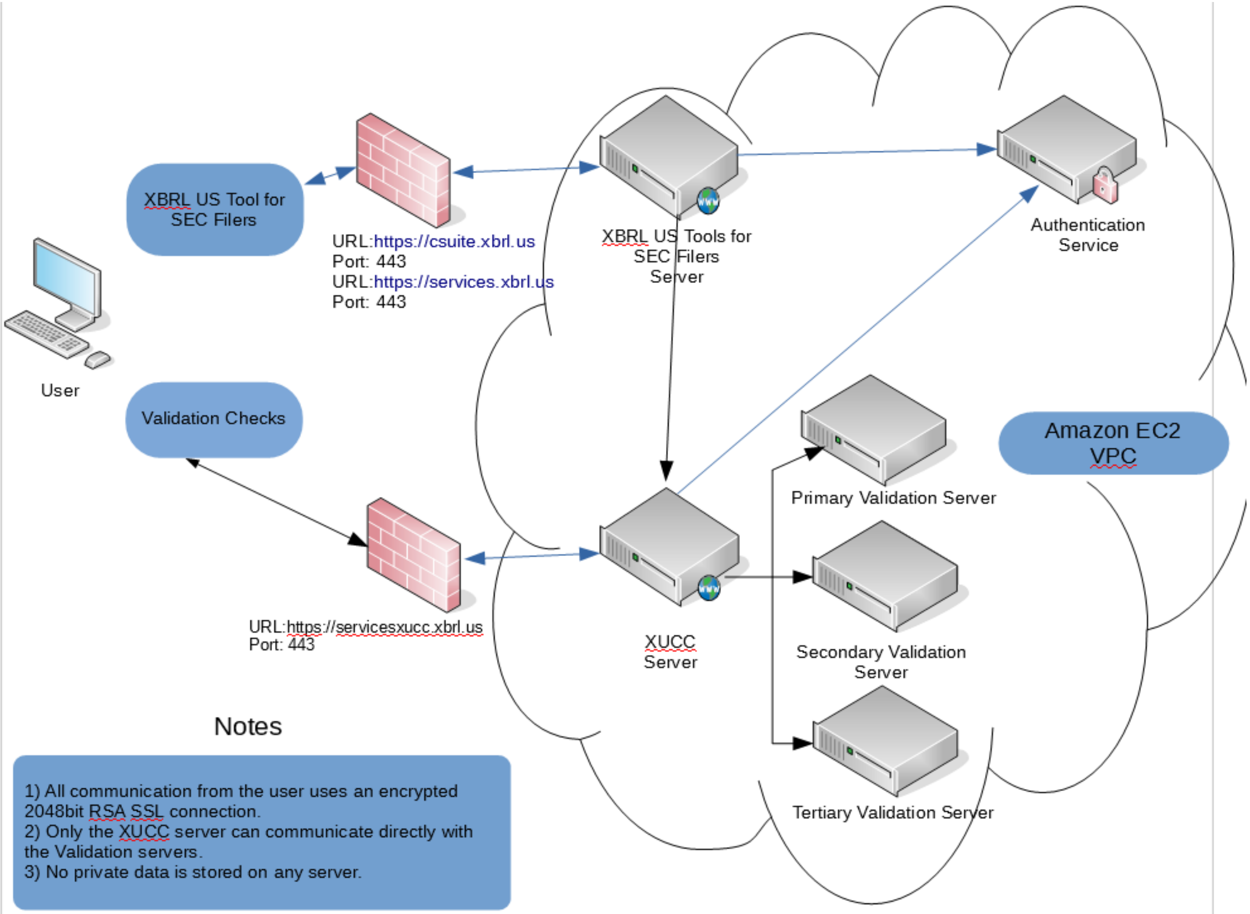
- XBRL US Flex application
- XBRL US Websites
- Web Service
- Third Party tools that support the consistency check service

In all cases, the connection to the validation checks must use a 2048-bit SSL connection. Upon receipt of the zip file, the user is authenticated to determine if the user submitting the request has the appropriate authorization to process the request. Upon successful authentication, the zip file is analyzed by the System to determine which taxonomy was used to create the filing. The filing is then read into the memory of the System and the appropriate Ruleset Checks service runs based on the taxonomy version. The filing is processed against the current rule set and any exceptions identified are returned to the user over a 2048-bit SSL connection. Upon receipt of the filing by the System, basic information is logged for monitoring and user troubleshooting purposes by XBRL US staff: the account ID making the request, the file name, the date of the submission, the taxonomy used, and any error messages are recorded if there is a failure processing the filing. No information is written and stored on disks other than this log information.

Infrastructure

Primary infrastructure, including the facilities, network, servers, and other equipment, used to provide XBRL US's System services is hosted by Amazon Web Services and located in the Amazon Cloud computer center.

The following describes the Amazon Cloud network topology:


XBRL US Tool for SEC Filers
URL:https://csuite.xbrl.us
Port: 443
URL:https://services.xbrl.us
Port: 443
XBRL US Tools for SEC Filers Server
Authentication Service
User
Validation Checks
Amazon EC2 VPC
Primary Validation Server
URL:https://servicesxucc.xbrl.us
Port: 443
XUCC Server
Secondary Validation Server
Tertiary Validation Server
Notes

1) All communication from the user uses an encrypted 2048bit RSA SSL connection.
2) Only the XUCC server can communicate directly with the Validation servers.
3) No private data is stored on any server.

Infrastructure

Primary infrastructure used to provide XBRL US Tools for SEC Filers services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
SEC Filer Tools Ruleset Server	Web server	Serves the System application to valid and authenticated users
XUCC Server	Application Server	As a component of the System application, this provides access the ruleset checks application
Primary, Secondary and Tertiary Validation Server	Application Server	As a component of the System application, this performs the filing validation processing

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Database Server	Application Server	As a component of the System application, this serves the public database used by the System application

Software

Primary software used to provide XBRL US Tools for SEC Filers services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
XBRL US Tools for SEC Filers Application	The main application that provides front end access to the public database and the ruleset checks	XBRL US Tools for SEC Filers Application
Validation Software	Provides an API for accessing and filing processing services	Validation Software

People

Company personnel provide support for the above services in each of the following functional areas:

- Corporate Administration - The President, assisted by the Vice President of Operations and Vice President of Communications, is responsible for overseeing strategic planning and corporate policy formulation. Administrative responsibilities include oversight of technology resources and service delivery performance and ensuring that these functional areas support the strategic goals and objectives of XBRL US
- Information Technology - The Applications Manager oversees the following functions: network design and implementation, technology selection and procurement, and software development and design. In addition, the Applications Manager manages monitoring network security and availability, computer operations, exception logs, and security and technology maintenance services. The IT infrastructure is under the direction of the President and Vice President of Operations
- Customer Service - The Vice President of Communications and Vice President of Operations oversee customer services, which takes responsibility for supporting the needs of customers on a day-to-day basis. They also monitor all incident reports and customer questions and complaints
- Rules Development - The President and Applications Manager are responsible for the development and testing of validation rules. They are also responsible for ensuring new rules are released for new taxonomies and that problems with rules are addressed on a timely basis

Processes

XBRL US has documented policies and procedures to support the operation and controls over its system. Specific examples of the relevant policies and procedures include the following:

- Employment Manual
- Standards of Business Ethics and Conduct
- Acceptable Use Policy
- Information Security Policy (including Security Instructions)
- Security Assessment Methodology
- Incident Response Policy

- Server & Desktop Decommissioning Policy
- Information Classification Policy
- System Development & Change Management Policy

The President of XBRL US utilizes the Monthly Control Checklist, which is used to ensure that all daily, weekly, and monthly management controls are performed in accordance with policy.

The Monthly Control Checklist is used to document the President's review that the following controls have been executed:

- Review of security policies and procedures
- Completion of risk assessment
- Review of any security events that have occurred and require communication with users
- Review of any security breaches that have occurred and resolution
- Listing of all major system changes
- Review of system changes for appropriateness
- Review of system changes and their impact on system security
- Completion of user access review
- Review of terminated employees and confirmation that access has been revoked
- Completion of annual network scans
- Review of user access logs
- Review of daily Samhain logs
- Current security policies and procedures are in place for the following items:
    - Security requirements of authorized users
    - Data classification
    - Risk assessment methodology
    - Prevention of unauthorized access
    - Maintenance of users
    - Responsibility of system security
    - Responsibility and accountability for system changes and maintenance
    - Testing, evaluating, and authorizing system components before implementation
    - Addressing how complaints and requests relating to security issues are resolved
    - Identifying and mitigating security breaches and other incidents
    - Providing for training and other resources to support system security policies
    - Exception handling
    - Meeting service level agreements and contractual requirements
    - Providing for sharing information with third parties

Physical Security

Physical and environmental controls are housed within AWS. For more information about their security control go to https://aws.amazon.com/security.

Logical Access

XBRL US, Inc 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 that identify and authenticate users and validate access requests against the users' authorized roles.

All resources are managed in a customer relationship system. The Company is responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to XBRL US, Inc resources using two-factor authentication. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality. Passwords must conform to defined password standards for the authentication system.

On an annual basis, access to resources are reviewed by the Applications Manager. In evaluating access, task requirements, duties requiring segregation, and risks associated with access are considered.

Computer Operations - Backups

System and customer authentication data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

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.

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

- Disk storage
- Network bandwidth

XBRL US, Inc has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. The Applications Manager reviews proposed operating system patches to determine whether the patches are applied. XBRL US, Inc 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. XBRL US, Inc staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

XBRL US, Inc maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

Development and testing are performed in an environment that is logically separated from the production environment. Information about changes are recorded and Management approves changes prior to migration to the production environment and documents those approvals within the approval system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation 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 that 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. Penetration testing includes network testing and occurs from outside (external testing) the network.

Data

The System does not record any data submitted to the system. All processed results are returned to the user. The only information stored is log information that contains no sensitive information, is secured, and is limited to authorized personnel.

Boundaries of the System

The scope of this report includes the Tools for SEC Filers System services provided by XBRL US at the Washington, D.C. location.

This report does not include the data center hosting services provided by Amazon Web Services.

Significant Events and Conditions

XBRL US has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the System services. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Preparation and Delivery of Reports and Data

XBRL US utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Subservice Organizations

The data center hosting services provided by Amazon Web Services are monitored by XBRL US, Inc.’s management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by Amazon Web Services:

Subservice Organization Controls		
Principle	**Criteria**	**Applicable Controls**
Common Criteria / Security	CC5.5	Physical access points to server locations are managed by electronic access control devices.
		Physical access to data centers is approved by an authorized individual.

Subservice Organization Controls		
Principle	**Criteria**	**Applicable Controls**
		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.

Criteria Not Applicable to the System

All Common criterion was applicable to the XBRL US Tools for SEC Filers System.

Significant Changes Since the Last Review

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

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 XBRL US's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of XBRL US'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 within the employment manual 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 security policies and procedures and understand their responsibility for adhering to the policies and procedures

Commitment to Competence

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

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

- Management has considered the requirements and responsibilities for particular jobs

Management's Philosophy and Operating Style

XBRL US'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 meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

XBRL US'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.

XBRL US'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.

Human Resources Policies and Practices

XBRL US'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. XBRL US'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 security policies and procedures following new hire orientation on their first day of employment
- New employees are required to submit to background check through HireRight that includes SSN validation/trace, widescreen plus national criminal search including 7-year criminal felony & misdemeanor history
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

XBRL US's risk assessment process identifies and manages risks that could potentially affect XBRL US'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. XBRL US 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 XBRL US, 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

XBRL US has established a 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. XBRL US attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

TRUST SERVICES PRINCIPLES AND CRITERIA

In-Scope Trust Services Principles

Common Criteria (*to the Security Principle)*
The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of XBRL US Tools for SEC Filers System services; as well as the nature of the components of the system result in risks that the criteria will not be met. XBRL US 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, XBRL US's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Although the trust services criteria and related controls are presented in section 4, "Information Provided by the Service Auditor," they are an integral part of XBRL US's system description.

Control Activities Specified by the Service Organization

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

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

MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. XBRL US'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

XBRL US management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. XBRL US monitors the following:

- Actual processing times against a maximum allowed processing time
- Availability of service
- Response times
- All processing failures
- Unauthorized changes to the server and application software

Reporting Deficiencies

The Monthly Control Checklist is utilized to document and track the results of on-going monitoring procedures.

INFORMATION AND COMMUNICATION SYSTEMS

Users gain access to the service using encrypted communications for both data submitted and received. Full time employees perform development and maintenance of all systems. XBRL US has implemented various methods of communication to ensure that employees understand their individual roles and responsibilities and that significant events are communicated in a timely manner. These methods include peered programming, ongoing periodic staff meetings, and training workshops, as needed. Every employee has a written job description that includes the responsibility to communicate significant issues and exceptions to an appropriate higher level of authority in a timely manner.

COMPLEMENTARY USER ENTITY CONTROLS

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

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles 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 XBRL US.
2. User entities are responsible for notifying XBRL US of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management, and control of the use of XBRL US services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize XBRL US services.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of XBRL US was limited to the Trust Services Principles and related criteria and control activities specified by the management of XBRL US and did not encompass all aspects of XBRL US'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 were performed using the following testing methods:

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

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

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

Control Activities Specified by the Service Organization

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security.	The entity evaluates its organizational structure, roles and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	Inspected the organizational chart to determine that the entity evaluated its organizational structure, roles and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed annually by management.	Inquired of the Applications Manager regarding the review of reporting relationships and organizational structure to determine that reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.
			Inspected the organizational chart versioning date to determine that the reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security.	The entity evaluates its organizational structure, roles and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	Inspected the organizational chart to determine that the entity evaluated its organizational structure, roles and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed annually by management.	Inquired of the Applications Manager regarding the review of reporting relationships and organizational structure to determine that reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.
			Inspected the organizational chart versioning date to determine that the reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and provides resources necessary for personnel to fulfill their responsibilities.	The entity evaluates its organizational structure, roles and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	Inspected the organizational chart to determine that the entity evaluated its organizational structure, roles and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to sign and accept the company's policies and procedures upon hire.	Inquired of the Applications Manager regarding the new hire process to determine that personnel were required to sign and accept the company's policies and procedures upon hire.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to sign and accept the company's policies and procedures upon hire.	No exceptions noted.
			Inspected the completed handbook forms for a sample of new hires to determine that personnel were required to sign and accept the company's policies and procedures upon hire.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
		Employees are required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	Inquired of the Applications Manager regarding the new hire process to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.
			Inspected the employee handbook to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security.	Personnel are required to sign and accept the company's policies and procedures upon hire.	Inspected the information security policies acknowledgement for a sample of new employees to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
			Inspected the information security policies acknowledgements for a sample of current employees to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.
			Inquired of the Applications Manager regarding the new hire process to determine that personnel were required to sign and accept the company's policies and procedures upon hire.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to sign and accept the company's policies and procedures upon hire.	No exceptions noted.
			Inspected the completed handbook forms for a sample of new hires to determine that personnel were required to sign and accept the company's policies and procedures upon hire.	Testing of this control activity disclosed that there were no newly hired employees during the review period.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	Common Criteria Related to Organization and Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Personnel are required to complete a background check provided by a third-party vendor upon hire.	Inquired of the Applications Manager regarding background checks to determine that personnel were required to complete a background check provided by a third-party vendor upon hire.	No exceptions noted.
			Inspected the employee manual to determine that personnel were required to complete a background check provided by a third-party vendor upon hire.	No exceptions noted.
			Inspected the completed background checks for a sample of new hires to determine that personnel were required to complete a background check provided by a third-party vendor upon hire.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Personnel are required to sign and accept the employee handbook and code of conduct upon hire.	Inquired of the Applications Manager regarding the new hire process to determine that personnel were required to sign and accept the employee handbook and code of conduct upon hire.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee handbook to determine that personnel were required to sign and accept the employee handbook and code of conduct upon hire.	No exceptions noted.
			Inspected the signed employee handbook acknowledgements for a sample of new hires to determine that personnel were required to sign and accept the employee handbook and code of conduct upon hire.	Testing of this control activity disclosed that there were no newly hired employees during the review period.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	System descriptions are communicated to authorized external users via service level agreements (SLA) that delineate the boundaries of the system and describe relevant system components.	Inspected the SLAs for a sample of clients to determine that system descriptions were communicated to authorized external users via service level agreements that delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel.	Inspected the company's shared network drive to determine that policy and procedures were documented for significant processes and available to personnel on the corporate intranet site.	No exceptions noted.
		A description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities is posted on the entity's website.	Inspected the company website to determine that a description of the entity's organization structure, system support functions, processes, and organizational roles and responsibilities were posted on the entity's website.	No exceptions noted.
		Customer responsibilities are outlined and communicated through service level agreements.	Inspected the SLAs for a sample of clients to determine that customer responsibilities were outlined and communicated through service level agreements.	No exceptions noted.
		A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	The entity's security commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Security commitments are communicated to external users via defined SLA.	Inspected the SLAs for a sample of clients to determine that security commitments were communicated to external users via defined SLA.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the company's shared network drive to determine that policies and procedures were documented for significant processes and available to personnel on the corporate intranet.	No exceptions noted.
		Employees are required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	Inquired of the Applications Manager regarding the new hire process to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.
			Inspected the employee handbook to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.

<table>
<tr><th colspan="5">COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES</th></tr>
<tr><th>CC2.0</th><th colspan="4">Common Criteria Related to Communications</th></tr>
<tr><th>Control Point</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the information security policies acknowledgement for a sample of new employees to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.</td><td>Testing of this control activity disclosed that there were no newly hired employees during the review period.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the information security policies acknowledgements for a sample of current employees to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Personnel are required to sign and accept the company’s policies and procedures upon hire.</td><td>Inquired of the Applications Manager regarding the new hire process to determine that personnel were required to sign and accept the company’s policies and procedures upon hire.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the employee handbook to determine that personnel were required to sign and accept the company’s policies and procedures upon hire.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the completed handbook forms for a sample of new hires to determine that personnel were required to sign and accept the company’s policies and procedures upon hire.</td><td>Testing of this control activity disclosed that there were no newly hired employees during the review period.</td></tr>
</table>

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the company's shared network drive to determine that policies and procedures were documented for significant processes and available to personnel on the corporate intranet.	No exceptions noted.
		Customer responsibilities are described on the entity's website and in user agreements.	Inspected the SLAs for a sample of clients to determine that customer responsibilities were described on the entity's website and in user agreements.	No exceptions noted.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.	Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected the monitoring tool to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
		Employees are required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	Inquired of the Applications Manager regarding the new hire process to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.
			Inspected the employee handbook to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security policies acknowledgement for a sample of new employees to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
			Inspected the information security policies acknowledgements for a sample of current employees to determine that employees were required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance.	No exceptions noted.
CC2.5	Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	The organization’s security policies and code of conduct are communicated to employees in the employee handbook.	Inspected the employee manual and the company’s internal shared drive to determine that the organization’s security policies and code of conduct was communicated to employees.	No exceptions noted.
		Documented incident response policies and procedures are in place and are available for review by employees on the secure network drive.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place and was available for review by employees on the secure network drive.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security are communicated to those users in a timely manner.	Defined SLA's are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security related failure, incidents, and concerns to personnel.	Inspected the SLAs for a sample of clients to determine that defined SLA's were in place and communicated to authorized external users. The SLA's included communication procedures for reporting security related failure, incidents, and concerns to personnel.	No exceptions noted.
		System changes are reviewed and approved by management prior to implementation.	Inspected the change approvals for a sample of changes to determine that system changes were reviewed and approved by management prior to implementation.	No exceptions noted.
		Changes are communicated to both internal and external users.	Inspected the internal change communication meeting and the external change communication to determine that changes were communicated to both internal and external users.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system security commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Inspected the master list of system components to determine that a master list of the entity's system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing the risk assessment process.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policy and the latest risk assessment to determine that management developed risk mitigation strategies to address all risks identified during the risk assessment process.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair security commitments and requirements.	Inspected the risk assessment policy and the latest risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security commitments and requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	Identified risks are rated using a risk evaluation process and rating are reviewed by management.	Inspected the risk assessment policy and the latest risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.
		Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy and most recent risk assessment to determine that management defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		External vulnerability scans are performed on a quarterly basis, and remedial actions are taken.	Inspected the network scan reports for a sample of quarters to determine that external vulnerability scans were performed on a quarterly basis, and remedial actions were taken.	No exceptions noted.
		Control self-assessments are performed by operating units on a monthly basis.	Inspected a sample of monthly control checklists to determine that control self-assessments were performed by operating units on a monthly basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC4.0	**Common Criteria Related to Monitoring of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Control self-assessments are performed by operating units on a monthly basis.	Inspected a sample of monthly control checklists to determine that control self-assessments were performed by operating units on a monthly basis.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring dashboard to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert application manager when thresholds have been exceeded.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that the monitoring software was configured to alert application manager when thresholds had been exceeded.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inquired of the Applications Manager regarding the new hire process to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the employee handbook to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the user access request tickets for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Applications Manager regarding the new hire process to determine that logical to systems was revoked to an employee as a component of the termination process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee handbook to determine that logical to systems was revoked to an employee as a component of the termination process. Inspected the user access revocation tickets and user listing for a sample of terminated employees to determine that logical to systems was revoked to an employee as a component of the termination process.	No exceptions noted. Testing of this control activity disclosed that there were no terminated employees during the review period.
	Network			
		Network user access is restricted via role based security privileges defined within the access control system.	Inspected the network user access listing and access rights to determine that network user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by the following personnel: • Application Manager	Inspected the network administrator access listing and access rights to determine that network administrative access was restricted to user accounts accessible by the following personnel: • Application Manager	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Complexity	Inspected the network authentication configuration to determine that system users were authenticated via individually-assigned user account and passwords. Production systems were configured to enforce password requirements that include: • Minimum length • Complexity	No exceptions noted.
		Network access reviews are completed by management on a quarterly basis.	Inspected the network access reviews for a sample of quarters to determine that network access reviews were completed by management on a quarterly.	No exceptions noted.
	Database			
		Database user access is restricted via role based security privileges defined within the access control system.	Inspected the database user access 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.
		Database administrative access is restricted to user accounts accessible by the following personnel: • Application Manager	Inspected the database administrator access listing and access rights to determine that database administrative access was restricted to user accounts accessible by the following personnel: • Application Manager	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application			
		Application user access is restricted via role based security privileges defined within the access control system.	Inspected the application user access listing and access rights to determine that application user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to user accounts accessible by the following personnel: • Application Manager	Inspected the application administrator access listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel: • Application Manager	No exceptions noted.
		Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the application authentication settings to determine that application users were authenticated via individually-assigned user accounts and passwords. The application was configured to enforce password requirements that include: • Password length • Complexity	No exceptions noted.
		Application access reviews are completed by management on a quarterly basis.	Inspected the application access reviews for a sample of quarters to determine that application access reviews were completed by management on a quarterly basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Remote Access			
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	VPN users are authenticated via multi-factor authentication (username, password, and public key) prior to being granted remote access to the system.	Inspected the VPN authentication to determine that VPN users were authenticated via multi-factor authentication (username, password, and public key) prior to being granted remote access to the system.	No exceptions noted.
		Privileged access to sensitive resources is restricted to defined user roles.	Inspected the network, database, and application user access listings and access rights to determine that privileged access to sensitive resources were restricted to defined user roles.	No exceptions noted.
		Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inquired of the Applications Manager regarding the new hire process to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the employee handbook to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the user access request tickets for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Applications Manager regarding the new hire process to determine that logical to systems was revoked to an employee as a component of the termination process.	No exceptions noted.
			Inspected the employee handbook to determine that logical to systems was revoked to an employee as a component of the termination process.	No exceptions noted.
			Inspected the user access revocation tickets and user listing for a sample of terminated employees to determine that logical to systems was revoked to an employee as a component of the termination process.	Testing of this control activity disclosed that there were no terminated employees during the review period.
		Control self-assessments are performed by operating units on a monthly basis.	Inspected a sample of monthly control checklists to determine that control self-assessments were performed by operating units on a monthly basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inquired of the Applications Manager regarding the new hire process to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the employee handbook to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the user access request tickets for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
		Control self-assessments are performed by operating units on a monthly basis.	Inspected a sample of monthly control checklists to determine that control self-assessments were performed by operating units on a monthly basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	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 access listing and access rights to determine that network user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by the following personnel: • Application Manager	Inspected the network administrator access listing and access rights to determine that network administrative access was restricted to user accounts accessible by the following personnel: • Application Manager	No exceptions noted.
		System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Complexity	Inspected the network authentication configuration to determine that system users were authenticated via individually-assigned user account and passwords. Production systems were configured to enforce password requirements that include: • Minimum length • Complexity	No exceptions noted.
		Network access reviews are completed by management on a quarterly basis.	Inspected the network access reviews for a sample of quarters to determine that network access reviews were completed by management on a quarterly.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database			
		Database user access is restricted via role based security privileges defined within the access control system.	Inspected the database user access 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.
		Database administrative access is restricted to user accounts accessible by the following personnel: • Application Manager	Inspected the database administrator access listing and access rights to determine that database administrative access was restricted to user accounts accessible by the following personnel: • Application Manager	No exceptions noted.
	Application			
		Application user access is restricted via role based security privileges defined within the access control system.	Inspected the application user access listing and access rights to determine that application user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to user accounts accessible by the following personnel: • Application Manager	Inspected the application administrator access listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel: • Application Manager	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password length • Complexity	Inspected the application authentication settings to determine that application users were authenticated via individually-assigned user accounts and passwords. The application was configured to enforce password requirements that include: • Password length • Complexity	No exceptions noted.
		Application access reviews are completed by management on a quarterly basis.	Inspected the application access reviews for a sample of quarters to determine that application access reviews were completed by management on a quarterly basis.	No exceptions noted.
	Remote Access			
		VPN users are authenticated via multi-factor authentication (username, password, and public key) prior to being granted remote access to the system.	Inspected the VPN authentication to determine that VPN users were authenticated via multi-factor authentication (username, password, and public key) prior to being granted remote access to the system.	No exceptions noted.
		Users can only access the system remotely through the use of the secure sockets layer (SSL), or other encrypted communication system.	Inspected the VPN authentication to determine that users could only access the system remotely through the use of secure socket layer (SSL), or other encrypted communication system.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is granted to an employee as a component of the hiring process.	Inquired of the Applications Manager regarding the new hire process to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the employee handbook to determine that logical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the user access request tickets for a sample of new hires to determine that logical access to systems was granted to an employee as a component of the hiring process.	Testing of this control activity disclosed that there were no newly hired employees during the review period.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Applications Manager regarding the new hire process to determine that logical to systems was revoked to an employee as a component of the termination process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee handbook to determine that logical to systems was revoked to an employee as a component of the termination process.	No exceptions noted.
			Inspected the user access revocation tickets and user listing for a sample of terminated employees to determine that logical to systems was revoked to an employee as a component of the termination process.	Testing of this control activity disclosed that there were no terminated employees during the review period.
		Control self-assessments are performed by operating units on a monthly basis.	Inspected a sample of monthly control checklists to determine that control self-assessments were performed by operating units on a monthly basis.	No exceptions noted.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC5.6	Logical access security measures have been implemented to protect against security threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Firewall systems are in place to filter inbound Internet traffic. Traffic not specifically permitted by a firewall rule is denied.	Inspected the network diagram and firewall rulesets to determine that a firewall system was in place to filter inbound traffic and deny any traffic not permitted by the firewall ruleset.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall rule set to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		Firewall rules limit the types of activities and service requests that can be performed from external connections.	Inspected the firewall rule sets to determine that firewall rules limited the types of activities and service requests that could be performed from external connections.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the SSL certificate 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 into the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security.	SSH, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity.	Inspected the encryption settings and certificates to determine that SSH, SSL, secure file transfer program (SFTP), and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Storage drives for workstations and laptops are encrypted.	Inspected the drive encryption configuration settings to determine that storage for workstations and laptops were encrypted.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security.	Access to implement changes in the production environment is restricted to authorized IT personnel.	Inspected the access rights to implement changes to the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		File integrity monitoring software is utilized to help detect unauthorized changes within the production environment.	Inspected the file integrity monitoring software configuration to determine that file integrity monitoring software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		Antivirus software is installed on production servers and workstations.	Inspected the antivirus software to determine that antivirus software was installed on production servers and workstations.	No exceptions noted.

<table>
<tr><th colspan="5">COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES</th></tr>
<tr><th>CC5.0</th><th colspan="4">Common Criteria Related to Logical and Physical Access Controls</th></tr>
<tr><th>Control Point</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Antivirus software is configured to update virus definitions on a real-time basis.</td><td>Inspected the antivirus update configurations to determine that antivirus software was configured to update virus definitions on a real-time basis.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Antivirus software is configured to perform quick scans daily and full system scans on a weekly basis.</td><td>Inspected the antivirus scan configurations to determine that antivirus software was configured to perform quick scans daily and full system scans on a weekly basis.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>External vulnerability scans are performed on a quarterly basis, and remedial actions are taken.</td><td>Inspected the network scan reports for a sample of quarters to determine that external vulnerability scans were performed on an annual basis, and remedial actions were taken.</td><td>No exceptions noted.</td></tr>
</table>

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	Vulnerabilities of system components to security breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security.	Logging and monitoring software is used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	Inspected the monitoring software configuration to determine that logging and monitoring software was used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert application manager when thresholds have been exceeded.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that the monitoring software was configured to alert application manager when thresholds had been exceeded.	No exceptions noted.
		Documented incident response policies and procedures are in place and are available for review by employees on the secure network drive.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place and was available for review by employees on the secure network drive.	No exceptions noted.
		Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.	Inspected the backup configurations and schedules to determine that incremental backups were performed on a daily basis, and full backups were performed on a weekly basis.	No exceptions noted.
		Antivirus software is installed on production servers and workstations.	Inspected the antivirus software to determine that antivirus software was installed on production servers and workstations.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is configured to update virus definitions on a real-time basis.	Inspected the antivirus update configurations to determine that antivirus software was configured to update virus definitions on a real-time basis.	No exceptions noted.
		Antivirus software is configured to perform quick scans daily and full system scans on a weekly basis.	Inspected the antivirus scan configurations to determine that antivirus software was configured to perform quick scans daily and full system scans on a weekly basis.	No exceptions noted.
		External vulnerability scans are performed on a quarterly basis, and remedial actions are taken.	Inspected the network scan reports for a sample of quarters to determine that external vulnerability scans were performed on an annual basis, and remedial actions are taken.	No exceptions noted.
		Firewall systems are in place to filter inbound Internet traffic. Traffic not specifically permitted by a firewall rule is denied.	Inspected the network diagram and firewall rulesets to determine that a firewall system was in place to filter inbound traffic and deny any traffic not permitted by the firewall ruleset.	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An automated backup system is utilized to perform scheduled system backups.	Inspected the backup configurations to determine that an automated backup system was utilized to perform scheduled system backups.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall rule set to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule set to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
CC6.2	Security incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Documented incident response policies and procedures are in place and are available for review by employees on the secure network drive.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place and was available for review by employees on the secure network drive.	No exceptions noted.
		Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.	Inspected the employee handbook to determine that entity policies included probation, suspension, and termination as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A ticket tracking application is utilized to track and respond to incidents.	Inquired of the Applications Manager regarding incident tracking to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.
			Inspected the incident response policy to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.
			Inspected the tickets for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents.	Testing of this control activity disclosed that there were no incidents during the review period.
		Resolution of events is communicated to users within the corresponding ticket.	Inquired of the Applications Manager regarding incident tracking to determine that resolution of events was communicated to both internal and external users within the corresponding ticket.	No exceptions noted.
			Inspected the incident response policy to determine that resolution of events was communicated to both internal and external users within the corresponding ticket.	No exceptions noted.
			Inspected the tickets for a sample of incidents to determine that resolution of events was communicated to both internal and external users within the corresponding ticket.	Testing of this control activity disclosed that there were no incidents during the review period.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	The entity's commitments and system requirements, as they relate to security are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	A documented SDLC is in place to guide personnel in the handling system changes.	Inspected the system development and change management policy to determine that a documented SDLC was in place to guide personnel in the handling of system changes.	No exceptions noted.
		System changes are reviewed and approved by management prior to implementation.	Inspected the change approvals for a sample of changes to determine that system changes were reviewed and approved by management prior to implementation.	No exceptions noted.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy and most recent risk assessment to determine that management defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair security commitments and requirements.	Inspected the risk assessment policy and the latest risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security commitments and requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	Common Criteria Related to Change Management			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security.	Identified risks are rated using a risk evaluation process and rating are reviewed by management.	Inspected the risk assessment policy and the latest risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policy and the latest risk assessment to determine that management developed risk mitigation strategies to address all risks identified during the risk assessment process.	No exceptions noted.
		A change management process is in place to guide personnel in the authorization, development, testing, approval, and implementation of system changes.	Inspected the system development and change management policy to determine that a change management process was in place to guide personnel in the authorization, development, testing, approval, and implementation of system changes.	No exceptions noted.
		Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented escalation procedures for reporting security incidents were in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Applications Manager regarding incident tracking to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the tickets for a sample of incidents 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 this control activity disclosed that there were no incidents during the review period.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security commitments and system requirements.	A documented SDLC is in place to guide personnel in the handling system changes.	Inspected the system development and change management policy to determine that a documented SDLC was in place to guide personnel in the handling of system changes.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the change tickets for a sample of changes to determine that system changes were tested prior to implementation and the types of testing performed depended on the nature of the change.	No exceptions noted.
		Changes are approved by management prior to implementation.	Inspected the change approvals for a sample of changes to determine that changes were approved by management prior to implementation.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inspected the access rights to implement changes to the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		File integrity monitoring software is utilized to help detect unauthorized changes within the production environment.	Inspected the file integrity monitoring software configuration to determine that file integrity monitoring software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**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 ticketing console and tickets for a sample of changes to determine that system change requests are documented and tracked in a ticketing system.	No exceptions noted.
		Changes are communicated to both internal and external users.	Inspected the internal change communication meeting and the external change communication to determine that changes were communicated to both internal and external users.	No exceptions noted.