A-LIGN

Professional Automation Services
Type 1 SOC 2
2018

AUTOMATING YOUR TAX PUZZLE SINCE 1986

PROFESSIONAL *AUTOMATION* SERVICES

REPORT ON PROFESSIONAL AUTOMATION SERVICES' DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on Service Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

December 15, 2018

Table of Contents

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT 1

SECTION 2 MANAGEMENT OF PROFESSIONAL AUTOMATION SERVICES' ASSERTION REGARDING ITS SYSTEM AS OF DECEMBER 15, 2018 4

SECTION 3 DESCRIPTION OF PROFESSIONAL AUTOMATION SERVICES' SYSTEM AS OF DECEMBER 15, 2018 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
CONTROL ENVIRONMENT 13
Integrity and Ethical Values 13
Commitment to Competence 14
Management's Philosophy and Operating Style 14
Organizational Structure and Assignment of Authority and Responsibility 14
Human Resources Policies and Practices 14
RISK ASSESSMENT 15
TRUST SERVICES PRINCIPLES AND CRITERIA 15
COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES 16
MONITORING 30
INFORMATION AND COMMUNICATION SYSTEMS 30
COMPLEMENTARY USER ENTITY CONTROLS 30

SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR 32

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 33

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT PROFESSIONAL AUTOMATION SERVICES RELEVANT TO SECURITY

To Professional Automation Services:

We have examined the attached description titled "Description of Professional Automation Services' Electronic Reporting Services System as of December 15, 2018" (the description) and the suitability of the design 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), as of December 15, 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 Professional Automation Services' ('PAS' or 'the Company') controls are suitably designed, 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.

PAS uses Nuvolat and CentriLogic ("subservice organizations") for colocation services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed. The description presents PAS' system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organizations expect to be implemented, and suitably designed at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations.

PAS has provided the attached assertion titled "Management of Professional Automation Services' Assertion Regarding Its Electronic Reporting Services System as of December 15, 2018," which is based on the criteria identified in management's assertion. PAS 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 PAS' assertion and on the suitability of the design 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 to meet the applicable trust services criteria as of December 15, 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 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 to meet the applicable trust services criteria. 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.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature and inherent limitations, controls at a service organization may not prevent, or detect and correct, all errors or omissions 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 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 PAS' assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented as of December 15, 2018, and
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 as of December 15, 2018, and user entities applied the complementary user-entity controls contemplated in the design of PAS's controls as of December 15, 2018 and the subservice organization applied, as of December 15, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.

This report is intended solely for the information and use of PAS; user entities of PAS' Electronic Reporting Services System as of December 15, 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

February 25, 2019
Tampa, Florida

SECTION 2

MANAGEMENT OF PROFESSIONAL AUTOMATION SERVICES' ASSERTION REGARDING ITS SYSTEM AS OF DECEMBER 15, 2018

Management of Professional Automation Services' Assertion
Regarding Its System as of December 15, 2018

February 25, 2019

We have prepared the attached description titled "Description of Professional Automation Services' Electronic Reporting Services System as of December 15, 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 Electronic Reporting Services 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 Electronic Reporting Services System as of December 15, 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 other parties, how such information is provided or received; the role of the 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 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.

Brian Anderson
President
Professional Automation Services

SECTION 3

DESCRIPTION OF PROFESSIONAL AUTOMATION SERVICES' SYSTEM AS OF DECEMBER 15, 2018

OVERVIEW OF OPERATIONS

Company Background

Professional Automation Services Inc. (PAS) was founded in April of 1985. PAS has been a data processing service provider and consulting company. Client companies have engaged PAS to provide software development and network consulting services. PAS started processing/printing/reporting of 1099 and W2 data in 1987. The tax compliance business has been providing growth capabilities to the company. Client company's engage PAS to print and mail W2/1099/W2/W2G/3921/1094/5-B/C forms to their employees. Certain companies further engage PAS to make available the W2/1099/1095/Paystubs forms available for self-service. Several companies host their pay stubs on one of PAS' web sites allowing the employee to receive their stub on-line. Employees also have the capability to self-select a notification capability: SMS or email of stub information. Companies make their W2s available through this web site as well.

Industries served by PAS include farming operations, staffing and temporary agencies, construction companies, church organizations and others.

Description of Services Provided

PAS provides the following services:

- W2 printing/mailing/hosting for web retrieval and federal, state and locality compliance reporting. PAS receives data from the client in various formats (csv, txt, Excel), processes the data applying edit criteria and then imports the data in to our database systems and then the client administrator(s) can verify data, run multiple management reports, request reprints and perform W2C editing. PAS can assist the client with federal, state and local compliance reporting
- 1095-B/C printing/mailing/hosting for web retrieval and IRS compliance reporting. Fully compliant with the ACA requirements for printing specifications and electronic submissions
- All 1099 forms, 1098, W2G, and 3921 printing/mailing/hosting for web retrieval and IRS reporting
- Monthly/quarterly unemployment insurance (SUI) reporting, 941/94x quarterly federal reporting
- Daily, monthly, quarterly deposit management
- Specialized data extraction export/import of wage data and unemployment reporting
- Software development and network consulting

Infrastructure

Primary infrastructure used to provide PAS's Electronic Reporting Services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewall/Router	Cisco ASA 5505	Provides firewall features and routing capabilities.
Servers	HP DL380 G7	Running VMWare VM machines that host the IVR system, web servers, load balancer.
Servers	HP DL580 G7	Running Hyper-V hosting for web servers and database systems.
Load Balancer	Load Balancer.org	Provides load balancing services for web server load management and through put.

Software

Primary software used to provide PAS's Electronic Reporting Services and internal infrastructure support system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Backup - Ultrabac	All Windows version	Provides workstation, server and VM backup.
Operating Systems	MS Windows server	Server 2008R2, Server 2012, Server 2016.
Visual Studio	2015, 2016, 2017	Development environment.
NetSparker	NetSparker	Web site vulnerability testing.
Jira	Issue tracking	Bug tracking and vulnerability testing issues and resolutions.
Support Center	Internal/external issue tracking	Communication method for employee updates on security seminars, etc. Provides a bug reporting system, assignment and resolution tracking.
NinjaRMM	Remote monitoring and management	Provides device management, reporting, updating and virus protection.
Provensec	Penetration testing	Provide external and internal penetration to identify and mitigate security leaks in the system.

People

PAS staff provide:

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

Processes and Procedures

Formalized IT policies and procedures exist in internal documentation as part of the employee manual, security policy manual and new hire procedures.

Physical Security

All remaining exterior ingress doors are restricted to users possessing a key that has been assigned access to use the door. Access to zones is restricted through the use of access control lists. Employees and vendors granted access keys are assigned to roles based on their job responsibilities.

Upon an employee's termination of employment, the HR system generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs before leaving the facility.

The premises are protected by a 24-hour monitored security system, that when triggered, delivers a notification to affected parties, including physical intrusion and panic alarms.

Logical Access

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

Customer employees access web site services through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Client Administrators are assigned passwords according to PAS password policies. Client employees self-create passwords (or are in the W2 information) with a complexity indicator on the web page. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with PAS's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Computer Operations - Backups

Customer 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 depending on customer indicated preference within the documented work instructions.

Backup infrastructure and on-site backup USB data media are physically secured in a locked fireproof safe. All backup data is encrypted. Media backups are rotated from the live environment to storage in the fire proof safe.

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.

PAS monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. PAS 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:

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

PAS has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. PAS staff review proposed operating system patches to determine whether the patches are applied. PAS system personnel are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. PAS staff validate that all patches have been installed and if applicable that reboots have been completed. In addition, the remote management and monitoring system notifies administrators system reboot management, system software updates and installation events, and additional application software events.

Change Control

PAS 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.

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

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

Data Communications

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

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event 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. PAS verifies that the third-party vendor uses accepted industry standard penetration testing methodologies correlated with industry standard promulgators like the Open Web Security Project.

(OWASP) and other security technology leaders. The third-party vendor's approach begins with a vulnerability analysis of the target system determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network (internal testing).

PAS identified a vendor that incorporated all of the identified security vulnerabilities for web sites and other public facing software applications. Rather than use a third-party service where testing has to be contracted on a reoccurring basis, PAS selected a vendor (NetSparker) that allows for PAS staff to conduct testing as frequently as needed and to incorporate web site vulnerability testing as part of the deployment processes when bugs are fixed, tickets are completed, or enhancements are installed. Testing is generally performed off hours or as needed if a major bug fix is determined for deployment is urgent.

Authorized employees may access the system through the Internet through the use of leading VPN or remote access technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured, processed and made available to Customers for verification, printing and portal availability. Such data includes, but is not limited to, the following:

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

Boundaries of the System

This report includes the Electronic Report Services provided by Professional Automation Services at the Longmont, Colorado facilities.

This report does not include the colocation services provided by Nuvolat and CentriLogic at the North Carolina facilities.

Significant Events and Conditions

PAS has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the security of the network systems and server systems. 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

PAS 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 colocation services provided by Nuvolat and CentriLogic are monitored by management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by Nuvolat and CentriLogic:

Subservice Organization Controls - Nuvolat & CentriLogic		
Principle	**Criteria**	**Applicable Controls**
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 and availability.	CC5.5	An ID card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.
	CC5.5	Visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.
	CC5.5	Visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.

Criteria Not Applicable to the System

All Common criterion was applicable to the PAS Electronic Reporting Services system.

Significant Changes Since the Last Review

No significant changes have occurred to the services provided to user entities since the 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 PAS's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of PAS's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

Commitment to Competence

PAS'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 competence levels for particular jobs and translated required skills and knowledge levels into written position requirements, these job requirements and skill sets have been communicated to HR and incorporated into the interview/hiring/evaluation processes
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

PAS'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.

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

Human Resources Policies and Practices

PAS'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. PAS'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:

- Any applicant for any position within the organization process during the interview process has to acknowledge and accept that a background check will be performed, as the background check results are evaluated the candidate will be advised if a second or more interview(s) will be required
- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment

- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

PAS’s risk assessment process identifies and manages risks that could potentially affect PAS’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. PAS 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 PAS, 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

PAS has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. PAS 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 PAS’s Electronic Reporting Services system; as well as the nature of the components of the system result in risks that the criteria will not be met. PAS 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, PAS’s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

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**
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.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed at least annually by management. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions at least annually and makes updates, if necessary.
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.	A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions at least annually and makes updates, if necessary.
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.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process. The experience and training of candidates for employment of transfer are evaluated before they assess the responsibilities of their position. Employee evaluations are performed for employees on an annual basis. Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance. Management documents skills and continued training to establish the organization's commitments and requirements for employees. Management tracks and monitors compliance with training requirements.

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**
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.	An information security policy has been documented that employees are required to read and acknowledge code of conduct to communicate workforce conduct standards and enforcement procedures. Personnel are required to sign and accept the code of conduct upon hire. Background checks are conducted on employee candidates before the onboarding process.

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**
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 agreement (SLA) that delineate the boundaries of the system and describe relevant system components. A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel. A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed as needed by management. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Customer responsibilities are outlined and communicated through service level agreements.
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. Policies and procedure are documented for significant processes are available on the entity's shared drive. Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance. Personnel are required to sign and accept the code of conduct upon hire.
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 are available on the entity's shared drive. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions as needed and makes updates, if necessary. Personnel are required to attend annual security and confidentiality training. Customer responsibilities are outlined and communicated through service level agreements.

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**
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. Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance.
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 and employees are required to acknowledge code of conduct upon hire. Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Defined SLAs are in place and communicated to authorized external users that delineate procedures for reporting security related failure, incidents, and concerns to personnel.
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.	System changes are authorized, tested, and approved by management prior to implementation. Changes are communicated to internal users. Changes are communicated to external users.

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**
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 (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use. Documented policies and procedures are in place to guide personnel when performing the risk assessment process. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and rating were reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
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.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. External vulnerability scans and penetration tests are performed on an annual basis and remedial actions are taken. Business continuity and disaster recovery plans are developed and updated on an as needed basis. Business continuity and disaster recovery plans are tested on an annual basis.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC4.0	**Common Criteria Related to Monitoring Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
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 that include, but are not limited to, risk assessments, and backup restoration tests are performed at least annually. Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert system administrator when thresholds have been exceeded.

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**
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. Logical and physical access to systems is granted to employees as a component of the hiring process. New hire access to resources is provisioned as requested in the new hire checklist. Logical and physical access to systems is revoked as a component of the termination process. Network user access is restricted via role-based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by authorized employees. Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Network account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Database user access is restricted via role-based security privileges defined within the access control system.

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
		Database administrative access is restricted to user accounts accessible by authorized employees. Database users are authenticated via individually-assigned user accounts and passwords. Databases are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Database account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by authorized employees. Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password length • Complexity Application account lockout policies are in place that include: • Timeout duration • Denied preload credentials • CAPTCHA configuration

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**
		Application audit policy configurations are in place that include: • Account logon events • Account management • Logon events • Object access • Privilege use • Process tracking • System events
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.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Account sharing is prohibited.
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. Logical and physical access to systems is granted to an employee as a component of the hiring process. Users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.
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. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process.
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.	Policies and procedures are in place to guide personnel in physical security activities. Management reviews third-party attestation reports annually. to ensure service level agreements are met.

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**
		Key assignment log is maintained for log of access to and within the office facility. Physical access to systems is granted to an employee as a component of the hiring process. Access to the server room is restricted to authorized employees. Entity has contracted with a third-party alarm company for security monitoring. Physical access privileges to the corporate office facility are revoked as a component of the termination process. Refer to the Subservice Organizations section above for additional controls managed by the subservice organization.
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.	A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.
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.	SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity. Backup media is stored in an encrypted format. Media is encrypted before being extracted from the system.
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.	Internal and external vulnerability scans and external penetration tests are performed on an annual basis. Antivirus software is installed on workstations to detect and prevent the transmission of data or files via dynamic threat detection. The antivirus software is configured to scan workstations on a daily basis.

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**
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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert system administrator when thresholds have been exceeded. Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Antivirus software is installed on workstations to detect and prevent the transmission of data or files via dynamic threat detection. The antivirus software is configured to scan workstations on a daily basis. The antivirus software provider pushes updates to the installed anti-virus software as new updates/signatures are available. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An automated backup system is utilized to perform scheduled system backups. Full backups of certain application and database components are performed on a weekly basis and incremental backups are performed on a daily basis. IT personnel monitor the success or failure of backups and are notified of backup job status via email notifications.
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 to guide personnel in the event of an incident. A ticket tracking system is utilized to track and respond to incidents. Resolution of events is communicated to users. Change management requests are opened for events that require permanent fixes.

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**
		Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.

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**
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.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. System changes are authorized, tested, and approved by management prior to implementation.
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. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
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.	Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints. A ticket tracking application is utilized to track and respond to incidents.
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.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. System change requests are documented and tracked in a ticketing system. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. Changes are approved by management prior to implementation. Changes are communicated to internal users. Changes are communicated to external users. Development and test environments are physically and logically separated from the production environment.

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**
		Access to implement changes in the production environment is restricted to authorized IT personnel. Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation.

MONITORING

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

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

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

Reporting Deficiencies

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

INFORMATION AND COMMUNICATION SYSTEMS

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

Specific information systems used to support PAS's Electronic Reporting Services system are described in the Description of Services section above.

COMPLEMENTARY USER ENTITY CONTROLS

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

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 PAS.
2. User entities are responsible for notifying PAS of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of PAS services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize PAS services.
6. User entities are responsible for providing PAS with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying PAS of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

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 PAS was limited to the Trust Services Principles and related criteria and control activities specified by the management of PAS and did not encompass all aspects of PAS' 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.