Attachment A

2019

AT-101 SOC 2 Type 2 Attestation Report

PREPARED FOR Permitium, LLC

Lazarus Alliance, Inc., Inc.
27743 N 70th ST Suite 100
Scottsdale AZ 85266 United States
http://www.lazarusalliance.com

05-10-2019

REPORT ON COMPANY'S DESCRIPTION OF ITS BUSINESS PLATFORM SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND EFFECTIVENESS OF ITS CONTROLS

Permitium, LLC

Assessment Dates: 05-01-2018 - 04-30-2019

Table of Contents

Section 1 - Assertion of Company's Service Organization Management

Illustrative Assertion by Service Organization Management

05-10-2019

Assertion of Permitium, LLC Service Organization Management

We have prepared the accompanying description in section 3 titled "Permitium, LLC Service Organization's Description of Its Software as a Service (SaaS) platform throughout the period May 1, 2018, to April 30, 2019" (description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria). The description is intended to provide report users with information about the Software as a Service (SaaS) platform that may be useful when assessing the risks arising from interactions with Permitium, LLC Service Organization's (Permitium, LLC) system, particularly information about system controls that Permitium, LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

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

a. the description presents Permitium, LLC hosted services system as of April 5, 2019, based on the following description criteria that was designed and implemented throughout the period May 1, 2018, to April 30, 2019, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period May 1, 2018, to April 30, 2019, to provide reasonable assurance that Permitium, LLC service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. the controls stated in the description operated effectively throughout the period May 1, 2018, to April 30, 2019, to provide reasonable assurance that Permitium, LLC service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2 - Independent Service Auditor's Report

Independent Service Auditor's Report

To: Permitium, LLC Service Organization

Assessment Scope

Lazarus Alliance, Inc. has examined Permitium, LLC ("Permitium", the "Company" or the "Service Organization") description of its Software as a Service (SaaS) offering, the suitability of the design of controls, and the operating effectiveness of controls during the assessment period from May 1, 2018 to April 30, 2019 to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design and operating effectiveness of Permitium, LLC controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls. Permitium, LLC uses the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) Infrastructure as a Service (IaaS) platform for clients' hosted production infrastructure and backup services. The description of the system in this report includes only the control objectives and related controls of Permitium, LLC and excludes the control objectives and related controls of the sub-service organizations. Our examination did not extend to controls of the Amazon Web Services (AWS) sub-service organization.

Service Organization's Responsibilities

Permitium, LLC has provided an assertion about the fair presentation of the description and the suitability of the design of the controls to achieve the related control objectives stated in the description. Permitium, LLC is responsible for preparing the description and for its assertion, including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives, selecting the criteria and designing, implementing and documenting controls to achieve the related control objectives stated in the description.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, 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, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description of assessment period. An examination of a description of a service organization's system and the suitability of the design of the service organization's controls to achieve the related control objectives stated in the description involves the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed and operating effectively to achieve the related control objectives stated in the description. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Management's assertion in this report. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Description of Tests of Controls

The specific controls reviewed are listed in section titled Control Objectives and Related Controls.

Assessors' Opinion

We have examined the attached description titled "Description of Permitium, LLC Software as a Service (SaaS) platform throughout the period May 1, 2018 to April 30, 2019 (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security and privacy principles set forth in TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria), throughout the period May 1, 2018 to April 30, 2019. 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 Permitium, LLC ('Permitium' 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. Permitium, LLC utilizes the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) Infrastructure as a Service (IaaS) platform for data center hosting services. Permitium, LLC control objectives and related controls, which are listed in Section 3 of this report, include only the control objectives and related controls of Permitium, LLC.

Permitium, LLC has provided the attached assertion titled "Management of Permitium's Assertion Regarding Its Business and Collaboration Application System throughout the Period May 1, 2018 to April 30, 2019," which is based on the criteria identified in management's assertion. Permitium, LLC 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 Permitium, LLC 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 May 1, 2018 to April 30, 2019.

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 Permitium, LLC assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period May 1, 2018 to April 30, 2019.

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 May 1st, 2018 to April 30th 2019, and user entities applied the complementary user-entity controls contemplated in the design of Permitium, LLC controls throughout the period May 1, 2018 to April 30, 2019.

c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period May 1, 2018 to April 30, 2019.

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 Permitium, LLC; user entities of Permitium, LLC Business and Collaboration Application System during some or all of the period May 1, 2018 to April 30, 2019; 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.

Lazarus Alliance Compliance, LLC and Lazarus Alliance, Inc. Scottsdale, Arizona

Restricted Use

This report and the description of the suitability of the design and operating effectiveness of controls in this report are intended solely for the information and use of Permitium, LLC Software as a Service (SaaS) platform system for the assessment period and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by user entities themselves, when assessing the risks and regulatory compliance of non-financial reporting controls. This report is not intended to be and should not be used by anyone other than those specified parties.

Sincerely,

Steve Tao, CPA
Lazarus Alliance Compliance, LLC - Proactive Cyber Security®
M: 888-896-7580 | F: 480-272-8846
Steve.Tao@LazarusAlliance.com
27743 N. 70th Street,
Suite 100,
Scottsdale, AZ 85266

Section 3 - Service Organization's Description of Its Business Platform System

Permitium, LLC's Assertion

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of Permitium, LLC controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions that may be affected by policies and procedures of Permitium, LLC SaaS platform. This report describes the system and control structure of Permitium, LLC as it relates to its SaaS platform. It is intended to assist Permitium, LLC customers and its independent auditors in determining the adequacy of the internal controls that are outsourced to Permitium, LLC and are relevant to customers' internal control structures as it relates to regulatory compliance risks. This document was prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants AT-101 Service Organization Control (SOC) 2 control framework. This description is intended to focus on the internal control structure of Permitium, LLC that is relevant to its SaaS platform customers only and does not encompass all aspects of the services provided or procedures followed by Permitium, LLC.

Management representative,

Jeff Maner

Client Services Director

04-05-2019

Company Overview and Services Provided

Permitium, LLC provides a suite of Software as a Service (SaaS) document management solutions on a subscription basis.

Principal Service Commitments and System Requirements

Permitium, LLC designs its processes and procedures related to application development to meet its organizational objectives. Those objectives are based on the service commitments that applications contain the functional elements required by clients while maintaining maximum security controls adhering to the laws and regulations that govern student information services, and the financial, operational, and compliance requirements that Permitium, LLC has established for the services. Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

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

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

Components of the System Used to Provide the Services

Infrastructure

The Permitium, LLC application platform is hosted on the Amazon Web Services platform (AWS), a fully-managed Infrastructure as Service (IaaS) and Platform as a Service (PaaS) offering from Amazon, Inc. Amazon Web Service is developed and managed by the AWS team, and provides a cloud platform based on machine virtualization. This means that customer code deployed to the Web Service platform is securely delivered to the Permitium, LLC client community. Every physical node in AWS has one or more virtual machines, also called instances, that are scheduled on physical CPU cores, are assigned dedicated RAM, and have controlled access to local disk and network I/O.

Software

PermitDirector is a Software as a Service (SaaS) application developed and maintained by Permitium, LLC in- house software engineering group. The software engineering group enhances and maintains the PermitDirector platform to provide services to clients. Permitium, LLC is not sold as an "on premises" solution. The PermitDirector web interface is a multiuser, web-based application that is used to collect inputs from users, process data, and provide visual representations of key metrics to clients. It also provides some specific performance reports to help them manage their work with PermitDirector. To access the site, clients must complete the onboarding process and be provided credentials provisioned based on job duties.

Permitium, LLC organizational structure provides the framework for how organization-wide objectives are planned, executed, controlled, and monitored. A relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Permitium, LLC develops an organizational structure contingent, in part, on its size and nature of activities. The responsibilities of key positions within Permitium, LLC are clearly defined in documented job descriptions and communicated. Individuals that hold key positions are experienced, knowledgeable, and have lengthy tenure with the company. Permitium, LLC organizational structure supports communication of information both up to leadership as well as down to support staff. Permitium, LLC organizational structure is comprised of three primary business units and several groups that work together when delivering their SaaS platform. The three business units consist of:

- Management team is responsible for the oversight and monitoring of the organization's strategic direction and is responsible for making final decisions that are pushed down to the leadership team and ultimately to team members.

- Leadership teams are responsible for the overall management, communications, direction, and implementation of the management team's strategic direction. The leadership team is directly responsible for production and manages the quality of services.

- Team members are responsible for executing on company tasks and managing the day-to-day service offerings of their respective departments.

Data

Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization. The data flow of Permitium, LLC networks is restricted to their wide area network that consists of their internal network, hosted production systems, and certain site-to-site connections. The Permitium, LLC network is configured with Virtual Local Area Networks (VLANs) to provide increased segmentation between different customer environments. Remote access and administration are restricted via secure shell (SSH) connections and restricted to internal personnel of Permitium, LLC. Customers connect to their production site via Secure Sockets Layer (SSL) web connection.

• User organizations are responsible for defining the communications method utilized to connect to Permitium, LLC systems (e.g., direct connections, over public networks, etc.).

• User organizations are responsible for defining the communications method that Permitium, LLC uses when connecting to their organizations internal network.

• User organizations are responsible for defining any encryption methodology utilized in relation to Permitium, LLC services.

Processes and Procedures

Management has developed and communicated client procedures to restrict logical access to the PermitDirector platform and its data. Review of procedures is performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches. Selection, documentation, and implementation of security controls. Performance of annual management self-assessments to assess security controls. Authorization, changes to, and termination of information system access. Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage

- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Control Environment

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions toward financial reporting (conservative or aggressive selection of alternative accounting principles and which accounting estimates are developed); and management's attitudes toward information processing and accounting functions and personnel. Permitium, LLC management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Security Management

Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals. Permitium, LLC information security is governed by their corporate information security policies and procedures that are documented and communicated to personnel on a regular basis. Their policies are based on only permitting access as necessary to enable personnel to perform job responsibilities. The infrastructure team is responsible for administering and implementing user and system level security and the security department is responsible for monitoring security to ensure policies are being adhered to.

• User organizations are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Permitium, LLC systems.

• User organizations are responsible for immediately notifying Permitium, LLC of any actual or suspected information security breaches, including compromised user accounts.

• User organizations are responsible for determining whether Permitium, LLC security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.

• User organizations are responsible for ensuring that user IDs and passwords are assigned only to authorized individuals and that the access roles assigned to the user account are appropriate.

• User organizations are responsible for notifying Permitium, LLC of any user accounts that need to be added or removed due to employee termination or transfer of job responsibilities.

• User organizations are responsible for securing the method to request and remove access to ensure that appropriate users are requesting access to Permitium, LLC systems.

Security Policies

The following security policies and related processes are in place for:

- Information Security Program Charter
- Data Privacy Program
- Acceptable Use
- Internal Audit
- Certificate Management
- Data Breach Response
- Disaster Recovery
- Fraud Mitigation and Response
- Incident Response
- Key Management
- Password Requirements
- Security Awareness
- User Account Administration
- Vendor Management

- Web Application Security

Personnel Security

Background checks are performed on new employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to Permitium, LLC procedures for accessing systems and sanctions for violating Permitium, LLC information security policy. Employees are instructed to report potential security incidents to the help desk.

Physical Security and Environmental Controls

The PermitDirector application is hosted on the AWS application platform environment, a fully-managed Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offering from Amazon Web Services which is physically located within Amazon Web Services Datacenter facilities. Physical and Environmental Security controls are operated by AWS.

Change Management

Control activities provide reasonable assurance that application and system software are developed and installed to effectively support application reporting requirements and changes are authorized and tested prior to production migration. Permitium, LLC system development life cycle (SDLC) consists of new development, ongoing modification with application and system support activities, and bug management. From initial change requests to the deployment of changes, the entire SDLC process is documented in Permitium, LLC change management system that systematically links to code under development. The SDLC requires formal business requirements, impact assessments, testing, and authorization of deployment procedures. User organizations are responsible for defining, approving, and performing user acceptance.

System Monitoring

An effective monitoring foundation is dependent on establishing an effective "tone at the top" of the organization and a high priority regarding effective internal controls. This requires that the top management team and the board of directors are involved in the evaluation process. Monitoring internal controls is dependent on the selection and utilization of evaluators, which have a solid baseline understanding of internal controls. They also need to have suitable capabilities, resources, and authority to conduct a meaningful assessment of internal controls. Permitium, LLC monitoring of internal controls is performed through application of both ongoing evaluations and separate evaluations. These ongoing evaluations ascertain whether the components of their internal controls over services provided continue to function as designed and intended. In addition, these evaluations facilitate identification of internal control deficiencies and evaluators communicate findings to appropriate officials responsible for taking corrective action. Permitium, LLC has continuous internal reporting, monitoring, and evaluations procedures in place to identify deviations from internal controls to effectively report these deficiencies to appropriate departments. Monitoring is a process of assessing risks linked to achieving operational objectives. This requires establishing a monitoring foundation consisting of procedures for evaluating risks to their user organizations. Monitoring activities include assessment of controls and reporting the results of the assessment together with any required corrective action steps. Permitium, LLC monitoring procedures include:

- Periodic evaluation and testing of controls by their security department
- Continuous monitoring programs built into information systems
- Analysis of and appropriate follow-up on operating reports or metrics that might identify anomalies indicative of a control failure
- Self-assessments by management regarding the tone they set in the organization and the effectiveness of their oversight functions
- Quality assurance reviews of the System Development Life Cycle (SDLC) and internal security requirements

Problem Management

Security incidents and other IT-related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Data Backup and Recovery

Control activities provide reasonable assurance that system data is regularly backed up and available for restoration in the event of processing error or unexpected interruptions. Permitium, LLC utilizes an automated backup system to schedule and perform daily and weekly backup activities. Backups are scheduled, monitored, and validated through restoration testing by Permitium, LLC infrastructure team.

System Account Management

Permitium, LLC has implemented role-based security to limit and control access within the PermitDirector application environment. Employees are granted logical access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts. Administrative access to the Permitium, LLC servers and databases is restricted to authorized employees. Unique user identification numbers, names, and passwords are required to authenticate all users to the PermitDirector environment, as well as to the facility services, and client reporting websites. Password parameters consist of the following:

- Contain at least eight (8) characters
- Contain both upper-case and lower-case letters
- Contain at least one (1) number
- Contain at least one (1) special character
- User accounts must be locked after five (5) unsuccessful authentication attempts
- Server-side user sessions must expire ten (10) hours following successful authentication regardless of user activity

Risk Assessment Process

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the service organization's system. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their

occurrence, and determining actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system. In order to identify the risk associated with each control objective, a risk level assessment is performed on the control activities found within the respective control objectives. For example, a control objective such as physical security is comprised of individual control activities. Each control activity is reviewed by management and departmental personnel to determine whether the ability to adhere to the control activity as stated exists and the probability that Permitium, LLC will maintain adherence using a scaling system of high, medium, and low. Management considers risks that can arise from both internal and external factors including:

Internal

- Potential human error
- Changes in the operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- Funding of critical projects and ongoing operations
- Disruption of information systems processing and the extent to which backup systems are available and can be implemented
- New business models, products, or activities
- Corporate restructurings

External

- Changes of customer needs
- Natural disasters
- Carrier and utility outages

- Competition within market
- Other privacy and processing rules and regulations

Information and Communication Systems

Throughout the organization, Permitium, LLC conducts daily, weekly, monthly, quarterly, and annual meetings to identify and address significant issues affecting the company's operations. Defined agendas, meeting minutes, and a corporate information system are established vehicles used for addressing and monitoring activities, accomplishments, and issues. As annual business development plans are established, annual meetings are held throughout the company to communicate defined goals and report results achieved. Monthly management meetings provide the vehicle for management to communicate and respond to operational tasks and issues. At all corporate levels, the company has established communication channels to promote and distribute information up and down the defined management structure.

Monitoring Controls

An effective monitoring foundation is dependent on establishing an effective "tone at the top" of the organization and a high priority regarding effective internal controls. This requires that the top management team and the board of directors are involved in the evaluation process. Monitoring internal controls is dependent on the selection and utilization of evaluators which have a solid baseline understanding of internal controls. They also need to have suitable capabilities, resources, and authority to conduct a meaningful assessment of internal controls. Permitium, LLC monitoring of internal controls is performed through application of both ongoing evaluations and separate evaluations. These ongoing evaluations ascertain whether the components of their internal controls over services provided continue to function as designed and as intended. In addition, these evaluations facilitate identification of internal control deficiencies and evaluators communicate findings to appropriate officials responsible for taking corrective action. Permitium, LLC has continuous internal reporting, monitoring, and evaluations procedures in place to identify deviations from internal controls to effectively report these deficiencies to appropriate departments. Monitoring is a process of assessing risks linked to achieving operational objectives. This requires establishing a monitoring foundation consisting of procedures for evaluating risks to their user organizations. Monitoring activities include assessment of controls and reporting the results of the assessment together with any required corrective action steps. Permitium, LLC monitoring procedures include:

- Periodic evaluation and testing of controls by their security department
- Continuous monitoring programs built into information systems
- Analysis of and appropriate follow-up on operating reports or metrics that might identify anomalies indicative of a control failure
- Self-assessments by management regarding the tone they set in the organization and the effectiveness of their oversight functions
- Quality assurance reviews of the System Development Life Cycle (SDLC) and internal security requirements

Changes to the System During the Period

No changes have occurred during the assessment period.

Section 4—Trust Services Category, Criteria, Related Controls, and Tests of Controls

AT-101 SOC 2 Type 2 Attestation Report

Contact Information

Client	
▪ Company name:	Permitium, LLC
▪ Company address:	P.O. Box 30012, #133 Laguna Niguel California 92607 United States
▪ Company URL:	https://www. permitium.com/
▪ Company contact name:	Jeff Maner
▪ Contact phone number:	7045823441
▪ Contact e-mail address:	jeff.maner@scribsoft.com
Assessor Company	
▪ Company name:	Lazarus Alliance, Inc.
▪ Company address:	27743 N 70th ST Suite 100 Scottsdale AZ 85266 United States
▪ Company website:	http://www.lazarusalliance.com
Assessor	
▪ Assessor name:	Dennis Hutton
▪ Assessor phone number:	18888967580
▪ Assessor e-mail address:	dennis.hutton@lazarusalliance.com
Assessor Quality Assurance (QA) Primary Reviewer	
▪ QA reviewer name:	Steve Tao
▪ QA reviewer phone number:	18888967580

▪ QA reviewer e-mail address:	steve.tao@lazarusalliance.com

Date and Timeframe of Assessment

▪ Date of Report:	05-10-2019
▪ Timeframe of assessment (start date to completion date):	05-01-2018 - 04-30-2019
▪ Identify date(s) spent onsite at the entity:	Remote Assessment
▪ Descriptions of time spent onsite at the entity and time spent performing remote assessment activities, including time spent on validation of remediation activities.	Lazarus Alliance, Inc. performs remote assessment activities with the client each month reviewing artifacts, collecting evidence, collaborating with employees and maintaining the overall assessment status. In addition, our review included the hosting companies SOC 2 Type 2 report.

Assessment Introduction

This report on the internal controls placed in operations and tests of operating effectiveness is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions of the user organizations' financial statement that may be affected by policies and procedures of the company's platform system. The examination was performed in accordance with the AICPA AT-101, "Reporting on Controls at a Service Organization".

Applicable Trust Services Criteria Relevant to Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.
Security refers to the protection of:

1. Information during its collection or creation, use, processing, transmission, and storage and

2. Systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of Permitium, LLC service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

The system description, control objectives, and related controls are the responsibility of company management. Lazarus Alliance, Inc.'s responsibility is to express an opinion that the system description was fairly presented and controls were suitably designed to achieve the control objectives specified in the Testing Matrices and were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by company's management, were achieved during the period of examination.

Control Environment

The control environment represents the collective effect of various components in establishing and enhancing the effectiveness of specific controls and mitigating identified risks. In addition to testing the design and operating effectiveness of the control activities in Section 4 of this report, our review also included tests of and consideration of the relevant components of the company's control environment over operations that support the company's platform system.

Our tests of the control environment included the following procedures to the extent we considered necessary to address management's relevant control environment and included the following:

- Obtaining an understanding of the company's organizational structure, including the segregation of duties, policy statements, and personnel policies.
- Discuss with management, operations, administrative, and other personnel who were responsible for developing and enforcing daily activities and requirements.
- Testing of oversight and company level controls on a sample basis to ensure key control environment activities were operating as described.

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by the company's management for the period in review. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved during the audit period. The nature of the tests conducted took into consideration the type of control testing and the evidential matter that was available to perform a test to determine the operating effectiveness.

Types of Tests Performed

- **Inquiry:** tests include the corroboration of relevant personnel to verify the knowledge and understanding of the describe control activity.
- **Observation:** tests include the physical observation of the implementation and application of or existence of specific controls.
- **Inspection:** tests include the physical validation of documents, records, configuration, or settings.

- **Re-performance:** tests include the reprocessing of transactions, procedures, and calculations to ensure the accuracy and completeness of the control description.

Sampling Approach

Lazarus Alliance, Inc. adheres to the principle of continuous auditing which is an automatic method used to perform audit activities, such as control and risk assessments, on a more frequent basis. Technology plays a key role in continuous audit activities by helping to automate the identification of exceptions or anomalies, analyze patterns within the digits of key numeric fields, review trends, and test controls, among other activities.

The "continuous" aspect of continuous auditing and reporting refers to the real-time or near real-time capability for financial information to be checked and shared. Not only does it indicate that the integrity of information can be evaluated at any given point of time, it also means that the information is able to be verified constantly for errors, fraud, and inefficiencies. It is the most detailed audit.

Each instance of continuous auditing has its own cadence. The time frame selected for evaluation depends largely on the frequency of updates within the accounting information systems. Analysis of the data may be performed continuously, hourly, daily, weekly, monthly, etc. depending on the nature of the underlying business cycle for a given assertion.

The Control Objectives (CO) are provided by Permitium, LLC for evaluation of controls relevant to Trust Services Principles and Criteria for Security (AICPA, Trust Services Criteria).

A **system** is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management specified requirements.

System components can be classified into the following five categories:

- **Infrastructure**. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile

devices, and telecommunications networks).

- **Software.** The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- **People.** The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- **Processes.** The automated and manual procedures.
- **Data**. The information used or processed by a system (transaction streams, files, databases, and tables).

This document presents the trust services principle and criteria for assessing the description and suitability of the design of the controls over a system relevant to the security of the system or the information processed by the system.

For each principle, there are detailed criteria that serve as benchmarks used to measure and present the subject matter and against which the subject matter is evaluated.

The **attributes of suitable criteria** are as follows:

- **Objectivity.** Criteria should be free from bias.
- **Measurability.** Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- **Completeness.** Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- **Relevance.** Criteria should be relevant to the subject matter.

Trust Services Criteria for Security

This supplement contains authoritative AICPA Assurance Services Executive Committee material.

The trust services criteria for security, availability, processing integrity, confidentiality, and privacy and the related points of focus in this supplement have been extracted from TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, fn 1 issued in April 2017

by the AICPA's Assurance Services Executive Committee. fn 2 The complete text may be found at www.aicpa.org/ cyber security risk management.

The following table presents the trust services criteria and the related points of focus for security, availability, processing integrity, confidentiality, and privacy, which are applicable to a SOC 2® examination. In the table, criteria and related points of focus that come directly from the Committee of Sponsoring Organizations of the Treadway Commission's 2013 Internal Control—Integrated Framework (COSO framework) fn 3 are presented using a normal font. In contrast, criteria and points of focus that apply to engagements using the trust services criteria are presented in italics.

Trust Services Principle Matrix

TSP ID	Trust Services Criteria and Points of Focus	Description of Permitium, LLC Service Organization's Controls	Testing Performed	Testing Results
	Control Environment			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**1.** Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical	The entity has documented the employee code of conduct and ethical standards which are reviewed, updated if applicable, and approved	No relevant exceptions noted.

		values to support the functioning of the system of internal control. **2.** Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners. **3.** Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct. **4.** Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner. **5.** Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to	by senior management annually. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Personnel, including contractors, are required to read and accept the employee conduct of conduct and ethical standards upon their hire and formally reaffirm them annually thereafter. Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	

		those standards, and addressing deviations in a timely manner.	interviews with key personnel. Management monitors personnel compliance with the entity's standards of business conduct and ethical standards through monitoring of customer and personnel complaints and the use of a dedicated mailbox for reporting ethics concerns or violations of the code of conduct. The code of conduct includes a sanctions policy for personnel who violate the code of business conduct and requires management to enforce the sanction policy. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The entity enforces its code of conduct and statement of security, confidentiality, and privacy practices. As	

			evidenced by standards of conduct violations reported directly to the ethics mailbox or identified by management are reviewed directly by senior compliance officers. Prior to employment, all personnel are verified against regulatory screening databases, including at a minimum, credit, criminal, and employment checks. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The entity takes into consideration the use of contractors and vendors in establishing the code of conduct and agreements with service providers or business partners. Contractors and vendors are evaluated against the code of conduct and vendors must acknowledge the	

			entity's code of conduct in agreements to perform services on behalf of the entity. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts:

element_87_09d9746cd2319d02dae632f60da82e5b-Organizational Assessment & Monitoring Standard.pdf
element_87_09d9746cd2319d02dae632f60da82e5b-Information Security Program Charter.pdf
element_87_09d9746cd2319d02dae632f60da82e5b-Employee Code of Conduct.pdf
element_87_9797e106581bb1339dedc1d2fd39aac9-Policy Review_khoa.pdf
element_87_0d69c06b763373d1c4fe77516c05b623-Service Level Agreement Standard.pdf
element_87_e55cb4baf2371b8809f553b5afa74c68-Vendor-User Agency Agreement (2018).pdf
element_87_e55cb4baf2371b8809f553b5afa74c68-scribbles-accept-use-acceptable-use-standard (1).pdf
element_87_e55cb4baf2371b8809f553b5afa74c68-scribbles-contract-mutual-nondisclosure-agreement (1).pdf element_87_e55cb4baf2371b8809f553b5afa74c68-Julia_Policy.pdf

CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**1.** Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations. **2.** Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action. **3.** Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making. **4.** Supplements Board Expertise—The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.	Roles and responsibilities of the board of directors as outlined in the Information Security Program Charter are segregated from the roles and responsibilities of management. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The entity's Organizational Assessment and Monitoring Standard establishes specific standards for the assessment and ongoing monitoring of risks to company information assets, and business processes associated with current organizational structure and current reporting relationships. The assessor verified compliance with this control objective through the examination of documentation and policies,	No relevant exceptions noted.

			direct observation, and interviews with key personnel. The board of directors includes independent members including the Chairman to maintain independence from management. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The Information Security Charter defines roles and responsibilities relevant to security. As evidenced by audits performed which are based on compliance frameworks with established security, availabliity, processing intergrity, confidentialy, and privacy requirements. The assessor verified compliance with this control objective through the	

			examination of documentation and policies, direct observation, and interviews with key personnel.	
Artifacts:  element_93_baee3f4eb103d5e6302ee77bf1d57347-Organizational Assessment & Monitoring Standard.pdf element_93_baee3f4eb103d5e6302ee77bf1d57347-Policy Acknowledgement Form.pdf element_93_baee3f4eb103d5e6302ee77bf1d57347-Risk Assessment & Monitoring Standard.pdf element_93_baee3f4eb103d5e6302ee77bf1d57347-Information Security Program Charter.pdf element_93_baee3f4eb103d5e6302ee77bf1d57347-Information Systems and Technology Security Policy.pdf element_93_94902c22c45de26e67bf3656ffa0132a-Privacy Policy.pdf				
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and	**1.** Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives. **2.** Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity	Inspected the entity's Organizational Assessment and Monitoring Standard and determined it establishes specific standards for the assessment and ongoing monitoring of risks to company information assets, business processes associated with current organizational structure, and current reporting	No relevant exceptions noted.

	responsibilities in the pursuit of objectives.	structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity. **3.** Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization. **4.** Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities. **5.** Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures,	relationships, infrastructure and external resources. Management and the board of directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives. As evidenced by the Information Security Program Charter, Organziational Chart, Organizational Assessment and Monitoring Standard which were revised during the assessment period. Job descriptions are reviewed by management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made to enable execution of authorities and responsibilities and flow of	

		reporting lines, authorities, and responsibilities.	information to manage the activities of entity. As evidenced by the job descriptions and Organizational Chart. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the organization and requirements relevant to security. As evidenced by the job descriptions, Organizational chart, Information Security Progam Charter, and the Organizational Assessment and Monitoring Standard.	

			The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration requirements relevant to security, availability, processing integrity, confidentiality, and privacy. As evidenced by the job descriptions, Organizational Chart, Information Security Progam Charter, Information Systems and Technology Security Policy, and the Privacy Policy. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	

			interviews with key personnel. The entity's customer-facing website, web interface, and the standard service agreement outline the security commitments and obligations of user entities. Roles and responsibilities for external party interaction and activity monitoring are defined in written job descriptions and communicated to personnel. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

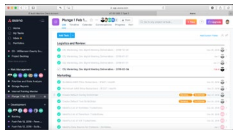
Artifacts:  element_102_a85c5242f7181a443056b4a2d79bdecc-Privacy Policy.pdf element_102_a85c5242f7181a443056b4a2d79bdecc-Customer Terms of Service.pdf element_102_a85c5242f7181a443056b4a2d79bdecc-Developer - Platform Job Description.pdf element_102_a85c5242f7181a443056b4a2d79bdecc-Developer - Intern Job Description.pdf element_102_a85c5242f7181a443056b4a2d79bdecc-Developer - Integration Job Description.pdf				
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**1.** Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives. **2.** Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings. **3.** Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to	Job requirements are documented in the organization's job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process to support the achievement of objectives. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization performs annual performance reviews	No relevant exceptions noted.

		support the achievement of objectives. **4.** Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control. **5.** Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. **6.** Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. **7.** Provides Training to Maintain Technical Competencies— The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	for employees and assesses the competencies and compliance of service providers during ongoing risk assessment. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Employees participate in mentoring and training programs and the organization has established requisite skillsets for personnel to support the achievment of objectives. Management has established a process for measuring personnel satisfaction during onboarding and in annual surveys to assess development directives to improve personnel retention. The assessor verified compliance with this control objective through the examination of documentation and policies,	

			direct observation, and interviews with key personnel. The organization has documented contingency plans for assignment of responsibility for internal controls. Contingency plans that address critical controls and processess are available to personnel on the intranet. The assessor verified the policy requirements and contingency planning related documentation through visual inspections and technical interviews with key personnel. The organization takes into account applicant backgrounds when determining whether to employ and retain employees and contractors. Prior to employment, personnel, including contractors, are verified against regulatory screening databases, including at a minimum, credit, criminal, and employment checks. As	

			evidenced by hiring policy/process, background checks, and job descriptions. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization takes into account all applicant's technical competencies when determining whether to employ and retain employees and contractors. Pre-employment screening includes technical interviews of applicants to determine their technical compentencies and ability to meet requirements in job descriptions. Technical compentencies are evaluated during annual performance reviews for existing personnel.	

			The assessor verified the policy requirements and contingency planning related documentation through visual inspections and technical interviews with key personnel. The organization provides training and continuing education programs to ensure the organization continues to develop skill sets and technical competencies and training resources are available. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts:  element_115_2b5463929d8821e9671fcaa093bc9646-Managment_Meeting_Agenda_CC8.1.pdf element_115_3eeb027c0df8649be0faa5878e689716-Staff Yearly Training Learning Plan.pdf element_115_3eeb027c0df8649be0faa5878e689716-Staff Development & Mentoring Process.pdf element_115_3eeb027c0df8649be0faa5878e689716-Management Mentoring Process.pdf element_115_781812fea1a5d9b8ef6888dd018121eb-Delivery Receipt.pdf element_115_781812fea1a5d9b8ef6888dd018121eb-RE_Clearance.pdf element_115_781812fea1a5d9b8ef6888dd018121eb-Comley.Certificate.CJIS Security Training.pdf				
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**1.** Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary. **2.** Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting	The organization has established structures, authorities, and responsibilites in the organization to communicate and hold individuals accountable for performing internal control responsbilities across the entity and implement corrective action as necessary. As evidenced by the Organizational Assessment and Monitoring Standard. The assessor verified compliance with this control objective through the	No relevant exceptions noted.

		appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives. **3.** Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives. **4.** Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance. **5.** Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or	examination of documentation and policies, direct observation, and interviews with key personnel. The organizaiton has a system in place to measure performance and award incentives for individuals at all levels of the organizaiton. Management has established measurable goals and performance criteria appropriate for responsibilities and objectives. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Leadership ensures performance incentives and rewards are aligned with internal control responsibilities in the achievement of objectives. Managment has established measurable goals and	

		exercise disciplinary action, as appropriate.	internal control responsibilities in the achievement of objectives. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Leadership ensures performance incentives and rewards are aligned with internal control responsibilities in the achievement of objectives. Managment has established measurable goals, performance criteria, considers pressures associated with the achievement of compliance, and internal control responsibilities in the achievement of objectives. The assessor verified compliance with this control objective through the examination of documentation and policies,	

			direct observation, and interviews with key personnel. Senior Management evaluates performance of internal control responsibilities, providing rewards and sanctions appropriate for responsibilities, considering the achievement of both short-term and longer-term objectives. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

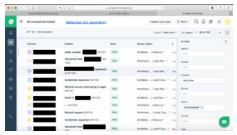
Artifacts:

element_132_d682d04d7ecd16344ad6e8192f4a6e79-Managment_Meeting_Agenda_CC8.1.pdf element_132_13680dc8f72a64e9cbd1b6b5f0020da0-● Priorities and Risks Analysis - CAB Meeting Agenda - 2019%2F01%2F21 - Asana.pdf element_132_13680dc8f72a64e9cbd1b6b5f0020da0-● Priorities and Risks Analysis - CAB Meeting Agenda - 2019%2F02%2F03 - Asana.pdf

element_132_1f3e5ed2743efc2982e334c07894f6c8-Organizational Assessment & Monitoring Standard.pdf element_132_7494cc00ee3a3f310859e905953d63e2-Training_Screenshot.pdf				
	Communication and Information			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**1.** Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives. **2.** Captures Internal and External Sources of Data—Information systems capture internal and external sources of data. **3.** Processes Relevant Data Into Information—Information systems process and transform relevant data into information. **4.** Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to	The organization performs an assessment at least annually to identify the information required and expected to support the internal control and the achievement of organization's service commitments and system requirements. The organization has established an Organizational Assessment and Monitoring Standard to evaluate the design and operating effectiveness of internal controls. The assessor verified compliance with this control objective through the examination of documentation and policies,	No relevant exceptions noted.

		assess its relevance in supporting the internal control components.	direct observation, and interviews with key personnel. The organization performs assessments at least annually to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements. The organization's most valuable and sensitive digital data and mission-critical systems are identified during the assessment, including internal and external sources of data. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization performs assessment at least annually to identify key information system processes that process relevant data into information to support the	

			internal control and the achievement of service commitments and system requirements. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has implemented processes and procedures relevant to internal audit to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts:  element_147_535353fc432c7e365e6d2df34c8f2182-Scribbles_Service Status_CC2.1.pdf element_147_535353fc432c7e365e6d2df34c8f2182-Scribbles_Contact_us_CC2.1.pdf element_147_33d1d85abb3cb63b372bf79bca8562bb-nist_800_30-itam-2018_1553209254.docx element_147_66cb155ee837446a89f68f38a6c8cb02-ector_isd_-_scribbles_signed.pdf element_147_082606f36d12d8bdcf5001e0fe716061-Safari - Mar 28, 2019 at 12_42 PM 3.pdf element_147_082606f36d12d8bdcf5001e0fe716061-Safari - Mar 28, 2019 at 12_42 PM.pdf element_147_082606f36d12d8bdcf5001e0fe716061-Safari - Mar 28, 2019 at 12_42 PM 2.pdf				
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the	1. Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities. 2. Communicates With the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	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. Policies and procedures as it relates to security of most valuable data and mission critical systems is available to	No relevant exceptions noted.

	functioning of internal control.	**3.** Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective. **4.** Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information. **5.** Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities. **6.** Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems	internal personnel on the intranet. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management meets at least quarterly to communicate information needed to fulfill their roles with respect to the achievement of organizations's service commitments and system requirements. As evidenced by the Organizational Assessment and Monitoring Standard. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management monitors personnel compliance with	

		failures, incidents, concerns, and other complaints to personnel. **7.** Communicates Objectives and Changes to Objectives —The entity communicates its objectives and changes to those objectives to personnel in a timely manner. **8.** Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program. **9.** Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation. **10.** Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	the entity's standards of business conduct and ethical standards through monitoring of customer and personnel complaints, and the use of a dedicated mailbox for reporting ethics concerns or violations of the code of conduct. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management monitors personnel compliance with the entity's standards of business conduct and ethical standards through monitoring of customer and personnel complaints, and the use of a dedicated mailbox for reporting ethics concerns or violations of the code of conduct with consideration for the timing, audience, and nature of the information.	

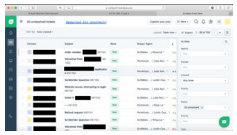
		11. Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.	The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The responsibilities of internal users whose roles affect system operation are communicated to those parties. Responsibilities and policies and procedures posted on entity's intranet are updated as necessary. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. Incident Response policies and	

			procedures includes escalation tree and communication plans depending on the nature of the incident, including escalation to senior management as necessary. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Changes to organizations's commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose services are part of the system. As evidenced by the organization's intranet, customer portal, and websites that document responsibilities, policies and procedures as it relates to security commitments and responsibilities are available to internal personnel on the intranet and external	

			personnel on organization websites and customer portals as applicable. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with security training requirements. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization provides information about the design and operation of the	

			system and its boundaries to appropriate personnel in order for them to understand their role in the system. Documentation is reviewed periodically to ensure it accurately reflects the system. As evidenced through system boundary documentation and communication to appropriate employees. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization provides information about the system objectives in order for them to understand their responsibilities in support of system operations. Documented responsibilities, policies and procedures as it relates to security commitments and responsibilities are available to internal personnel on the	

			intranet and external personnel on websites and customer portals as applicable, and that those responsibilities, policies and procedures documented history of changes with the date of change. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Planned changes to system components are reviewed, scheduled, and communicated to management as part of the system maintenance process. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel	

Artifacts:  element_158_7a3980b5bf704346d0c39d4fe8a55db2-Scribbles_Contact_us_CC2.1.pdf element_158_5e3c3f7a8bab311fd306dc806317fc7d-Information Security Incident Response Plan.pdf element_158_7d4413d377fe9aef2ad3a33d6021905c-Organizational Assessment & Monitoring Standard.pdf				
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**1.** Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties. **2.** Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.	The organization has proccesses in place to communicate relevant and timely information to external parties regarding the functioning of internal control. The organization is subject to relevant parties. As evidenced by communication of SOC 2 report or other communication of any audit findings. The assessor verified compliance with this control objective through the examination of	No relevant exceptions noted.

		3. Communicates With the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors. **4.** Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective. **5.** Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations. **6.** Communicates Objectives Related to Confidentiality and Changes to Objectives— The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.	documentation and policies, direct observation, and interviews with key personnel. The organization allows for inbound communications from customers, consumers, suppliers, external auditors, regulators, and others via reporting mechanisms on the organization's website. As evidenced by external reporting on the organization's website (i.e, 'Contact Us' section), and documented processes for triaging inbound communications. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Leadership meets at least quarterly to provide relevant information resulting from assessments	

		7. Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives related to privacy and changes to those objectives. **8.** Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation. **9.** Communicates System Objectives—The entity communicates its system objectives to appropriate external users. **10.** Communicates System Responsibilities—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have	conducted by internal and external parties. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management monitors personnel compliance with the entity's standards of business conduct and ethical standards through monitoring of customer and personnel complaints, and the use of a dedicated mailbox for reporting ethics concerns or violations of the code of conduct. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior management takes into account timing,	

		the information necessary to carry out those responsibilities. **11.** Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	audience and nature of communication and legal, regulatory, and fidcuciary requirements and expectations when communicating regarding the operating of internal control. The leadership team collaborates and ensures the team is aligned on the communication strategy, should external communication be necessary as evidenced by the Organizational Assessment and Monitoring Standard. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization disseminates changes to objectives related to confidentiality to external users as necessary. As evidenced by customer portal and websites that	

			document responsibilities as it relates to confidentiality, commitments, and responsibilities are available to external personnel. Agreements with the service providers and business partners outline the entity's requirements, including terms, conditions, and responsibilities. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has a privacy policy that is communicated externally via the company's website. Additionally, the organization has customer and vendor agreements in place that identify vendors any time there are changes to privacy objectives. The assessor verified compliance with this control objective through the	

			examination of documentation and policies, direct observation, and interviews with key personnel. The organization provides information about the design and operation of the system and its boundaries to external users in order for them to understand their responsibilities in the system and results of system operation. As evidenced by the organization's website and customer portal descriptions of the system, system boundaries, and system processes. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization provides information about the system objectives to appropriate external users in order for them to understand	

			their responsibilities in the system and results of system operation. As evidenced by the entity's customer portal and websites which document responsibilities as it relates to system objectives are available to external users. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. External users involved in any part of internal controls (developing, implementing, operating, monitoring) receive information necessary to carry out these responsibilities. The organization provides information about the system objectives to appropriate external users in order for them to understand their responsibilities in the system and results of system operation.	

			The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns, and complaints are available on the organization's website and system documentation. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts: element_183_2c9c91251cfee455bcbd9d5e6e62ea77-Safari - Mar 28, 2019 at 12_42 PM 3 (2).pdf element_183_2c9c91251cfee455bcbd9d5e6e62ea77-Safari - Mar 28, 2019 at 12_42 PM (2).pdf element_183_2c9c91251cfee455bcbd9d5e6e62ea77-Safari - Mar 28, 2019 at 12_42 PM 2 (1).pdf element_183_2c9c91251cfee455bcbd9d5e6e62ea77-ector_isd_-_scribbles_signed (1).pdf				
	Risk Assessment			
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**Operations Objectives** **1.** Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity. **2.** Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives. **3.** Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	Senior management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of Senior Leadership. The objectives incorporate the service commitments and system requirements of the organization. As evidenced by the annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	No relevant exceptions noted.

		4. Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance. **External Financial Reporting Objectives** **5.** Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances. **6.** Considers Materiality—Management considers materiality in financial statement presentation. **7.** Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions. **External Nonfinancial Reporting Objectives** **8.** Complies With Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and	interviews with key personnel. Senior leadership articulates the organization's risk appetite related to the achievement of operations objectives. The risk appetite is considered as part of the organization's annual business planning objectives to ensure alignment. As evidenced by the annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. As part of the annual business planning process, Senior Leadership defines operational and financial objectives. The objectives are reviewed and updated as appropriate throughout the year. The assessor verified compliance with this control	

		frameworks of recognized external organizations. **9.** Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting. **10.** Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits. **Internal Reporting Objectives** **11.** Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity. **12.** Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Resources are allocated taking into account the organization's operations objectives and associated performance during the organizations annual business planning process and budget decisions. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The assesor validated that the organization currently, as a non-publicly traded company, does not have responsibilities nor obligations to prepare and disclose financial statements	

		13. Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits. **Compliance Objectives** **14.** Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives. **15.** Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives. **16.** Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.	for external financial reporting objectives. The assesor validated that the organization currently, as a non-publicly traded company, does not have responsibilities nor obligations to prepare and disclose financial statements for external financial reporting objectives. The assesor validated that the organization currently, as a non-publicly traded company, does not have responsibilities nor obligations to prepare and disclose financial statements for external financial reporting objectives. Management establishes compliance objectives consistent with laws and regulations or standards and frameworks of recognized external organizations. The organization has established an audit program which includes assessments performed by external	

			auditors to assess compliance with laws, regulations, and frameworks. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established an Organizational Assessment and Monitoring standard to assess compliance with laws, regulations, and extrernal frameworks which are the basis of internal and external audits. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. External assessments of the organization conducted by	

			external auditors reflect underlying transactions and events within a range of acceptable limits for the applicable reporting period of the assessment. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization's internal audit program has been established to provide Senior Management with information to identify problems with the mitigation of identified risks, design of internal procedures, and execution of procedures by staff. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	

			interviews with key personnel. The organization has established an Organizational Assessment and Monitoring Standard to assess compliance with laws, regulations, and extrernal frameworks which are the basis of internal audits and assessments. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Internal assessments of the organization reflect underlying transactions and events within a range of acceptable limits for the applicable reporting period of the assessment. The assessor verified compliance with this control objective through the examination of documentation and policies,	

			direct observation, and interviews with key personnel. The organization takes into account laws and regulations in creating the standards of conduct. The standards of conduct are reviewed regularly to ensure it reflects business operations and compliance objectives. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior leadership articulates the organization's risk appetite related to the achievement of compliance objectives. The risk appetite is considered as part of the organization's annual business planning objectives to ensure alignment. As evidenced by the annual risk assessment report	

			and business planning documentation. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management identifies sub-objectives relating to security, availability, processing integrity, confidentiality, and privacy to support the acheivement of the entity's compliance objectives. As evidenced by the annual risk assessment report and annual business planning documentation. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts: element_210_c0e47887349266c345405e9c39ae00e0-nist_800_30-itam-2018_1553209254.docx element_210_4891d351ae5fd355207a70d687684c1b-Risk Assessment & Monitoring Standard.pdf element_210_4891d351ae5fd355207a70d687684c1b-ISO 27001 Compliance Matrix.pdf element_210_45d4906f53626f7b5366d8592d221c26-Scribbles and Permitium LLC CPA letter.pdf				
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**1.** Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives. **2.** Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives. **3.** Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.	Senior management meets to discuss strategy, operations, risk considerations, and other factors critical to the business on a periodic basis. Assessments are performed using a risk-based approach on a cadence appropriate for each control activity. As evidenced by the annual risk assessment report and the Organizational Assessment & Monitoring Standard. The assessor verified compliance with this control objective through the examination of documentation and policies,	No relevant exceptions noted.

		4. Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk. **5.** Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk. **6.** Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets. **7.** Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties—The entity's risk	direct observation, and interviews with key personnel. An annual risk assessment is performed to identify risks arising from external and internal sources and the effectiveness of these controls are shared with Senior Leadership. As evidenced by the annual risk assessment and penetration testing reports. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. An overview of the annual risk assessment is presented to Senior Leadership as well as used to help establish the annual assessment plan. The assessor verified compliance with this control objective through the examination of documentation and policies,	

		assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems. **8.** Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	direct observation, and interviews with key personnel. The organization assess and responds to security risks on an ongoing basis through regular management meetings with IT personnel, reviewing and acting upon security event logs, and conducting a formal annual risk assessment. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. During the annual risk assessment process, risk recommendations regarding whether to accept, avoid, reduce or share risks are identified. Management reviews the documented impact and liklihood of the risk. As evidenced by the annual risk assessment report	

			and business planning documentation. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization identifies critical assets in order to assist with identifying and responding to risks. The organization identifies threats and vulnerabilities through vulnerability scanning and responds accordingly. As evidenced by the annual risk assessment and vulnerability assessment reports. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

			As part of the organization's risk assessment process, the organization considers potential threats from vendors, business partners, customers and others with access to the entity's data. As evidenced by the annual risk assessment report and vulernability assessment reports. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The risk assessment process takes into account the potential impact of identified risks and determines the criticality of identified threats in meeting objectives. This includes assessing the impact of identified threats, determining the risk associated with assets based on asset criticality, and threat impact and	

			likelihood. The risk assessment is conducted annually and updated as needed. As evidenced by the annual risk assessment and vulnerability assessment reports. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts:

element_245_49af617af93c718614865a8612fa4494-nist_800_30-itam-2018_1553209254.docx
element_245_c06d47515299e664fb654161370586e2-penn-testing-03202019.pdf
element_245_abc8bf3bef0463bbb6b310b7b99b4b4b-Vulnerability Management Standard.pdf
element_245_abc8bf3bef0463bbb6b310b7b99b4b4b-Threat Assessment & Monitoring Standard.pdf
element_245_abc8bf3bef0463bbb6b310b7b99b4b4b-Risk Assessment & Monitoring Standard.pdf
element_245_abc8bf3bef0463bbb6b310b7b99b4b4b-ISO 27001 Compliance Matrix.pdf
element_245_c39ae392188c4d0a3d3b9cde704f5b28-Review.pdf

CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**1.** Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur. **2.** Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures. **3.** Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts. **4.** Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions. **5.** Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.	During the annual risk assessment process and internal audits, the organization considers the existence of fraud in the environment. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Management reviews the organization's compensation and performance programs annually to identify potential incentives and pressures for employees to commit fraud. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	No relevant exceptions noted.

			The organization has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management uses information technology tools including security systems, monitoring systems, and incident tracking systems to identify and manage fraud risk. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The annual risk assessment process takes into account	

			the fraud risks including consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information. The organization performs access control reviews on at least a quarterly basis. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	
Artifacts: element_264_a0e124818dab30b703e1c71e562e3f5d-nist_800_30-itam-2018_1553209254.docx element_264_756abdef8942fe9e1978ad5fbe6cc097-Scribbles and Permitium LLC CPA letter.pdf				
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could	**1.** Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical	The risk management process takes into account changes to regulatory, economic, and physical environment conditions. These factors are considered	No relevant exceptions noted.

	significantly impact the system of internal control.	environment in which the entity operates. **2.** Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. **3.** Assesses Changes in Leadership—The entity considers changes in management and respective attitudes and philosophies on the system of internal control. **4.** Assess Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment. **5.** Assess Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.	and documented as appropriate. As evidenced by the annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Leadership considers changes in management and strategy in internal audit program as appropriate. As evidenced by the Organizational Assessment & Monitoring Standard, Risk Assessment and Monitoring Standard, and annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

			Senior Leadership considers changes in management and strategy in internal audit program as appropriate. As evidenced by the Organizational Assessment & Monitoring Standard and the Risk Assessment and Monitoring Standard. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The risk assessment process takes changes in the organization's systems and technology environment into account. Risk assessments occur annually and information is reviewed for significant changes to the organization's systems and technology. As evidenced by the Organizational Assessment & Monitoring Standard, Risk Assessment and Monitoring	

			Standard, and annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. During the annual risk assessment process, the organization considers changes in vendor and business partner relationships. This includes but is not limited to ensuring vendors/business partners continue to provide the level of service agreed upon and maintain compliance with regulatory frameworks/standards. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts: element_277_4d9579ae64a2a043f9e09b70fa0a60db-nist_800_30-itam-2018_1553209254.docx element_277_1388cd90e6ce8831101642dc26ca2053-Vulnerability Assessment & Management Standard.pdf element_277_1388cd90e6ce8831101642dc26ca2053-Threat Assessment & Monitoring Standard.pdf element_277_1388cd90e6ce8831101642dc26ca2053-Risk Assessment & Monitoring Standard.pdf element_277_1388cd90e6ce8831101642dc26ca2053-Organizational Assessment & Monitoring Standard.pdf				
	Monitoring Activities			
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present	**1.** Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations. **2.** Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations. **3.** Establishes Baseline Understanding—The design and current state of an	The orgnizations has established an Organizational Assessment and Monitoring standard to perform periodic audits to including information security assessments. As evidenced by annual risk assessment reports, vulnerability assessments, and external assessments.	No relevant exceptions noted.

	and functioning.	internal control system are used to establish a baseline for ongoing and separate evaluations. **4.** Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated. **5.** Integrates With Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions. **6.** Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk. **7.** Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback. **8.** Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO	The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Organizational assessments include a risk analysis of all significant operating and reporting areas of the organization as a means to prioritize audit efforts for the year. As evidenced by the Organizational Assessment & Monitoring Standard, Risk Assessment and Monitoring Standard, vulnerability assessment reports, and annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has developed, documented,	

		certifications), and internal audit assessments.	and maintained a baseline configuration of the internal control system. As evidenced by the Organizational Assessment & Monitoring Standard, Risk Assessment and Monitoring Standard, vulnerability assessment reports, and annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization maintains job descriptions that articulate the background and knowledge personnel must possess to perform assessments in accordance with the Organizational Assessment & Monitoring Standard. The assessor verified compliance with this control objective through the examination of	

			documentation and policies, direct observation, and interviews with key personnel. The organization has established an Organization Assessment and Monitoring standard to perform ongoing evaluations that integrate with business processess and adjust to changes in the business environment. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management varies the scope and frequency of targeted assessments using a risk-based approach on the impact strategies and identification of targeted assessments. The assessor verified compliance with this control objective through the	

			examination of documentation and policies, direct observation, and interviews with key personnel. External auditors are employed to perform control testing to provide objective feedback regarding the design and operation of internal controls. As evidenced by third party control testing. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel Management performs a variety of ongoing and separate evaluations, including but not limited to vulnerability assessments, third party attestation reporting, and internal control activities (both ongoing and separate evaluations). Control deviations are	

			communicated to relevant stakeholders as appropriate. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	
Artifacts: element_292_e3f7b8bd2090440f2201abcc8632298b-nist_800_30-itam-2018_1553209254.docx element_292_5f300ce0f98f0023d878eb744dea9195-penn-testing-03202019.pdf element_292_890c53f9d8f174ab7cca5617b59086eb-CAB1 (1).pdf element_292_890c53f9d8f174ab7cca5617b59086eb-Review (1).pdf				
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for	**1.** Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations. **2.** Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior	Complete reports of deficiencies from internal and external sources are provided directly to Senior Leadership. Senior Leadership works with management to suggest appropriate remediation and follow up to ensure that	No relevant exceptions noted.

	taking corrective action, including senior management and the board of directors, as appropriate.	management and the board of directors, as appropriate. **3.** Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	proper controls have been established. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established an Organizational Assessment and Monitoring Standard that requires all deficiencies including serious threats to be reported directly to Senior Leadership. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Leadership tracks the status of all deficiencies that have been rated as a serious threat to the	

			organization until satisfactorily resolved. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	
Artifacts: element_311_ea6a2680e69fe472137c4441d8f61292-Review.pdf element_311_e59e322502af5122568da9fb70a0b42f-CAB1.pdf				
	Control Activities			
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to	**1.** Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out. **2.** Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is	No relevant exceptions noted.

	the mitigation of risks to the achievement of objectives to acceptable levels.	scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities. **3.** Determines Relevant Business Processes—Management determines which relevant business processes require control activities. **4.** Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. **5.** Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity. **6.** Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.	identified, management develops the requirements for the new controls and uses the change management process to implement them. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. As part of the risk assessment, management assessed the environment, complexity, nature, and scope of its operations when developing control activities to mitigate the risks. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established an	

			Organizational Assessment and Monitoring Standard to identify business processes that may require controls. These processes are reviewed and approved by Senior Management. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization's control framework includes a variety of controls that address risks. The organization leverages preventive and detective controls, as well as manual and automated controls to ensure they are designed and operating effectively. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	

			interviews with key personnel. The organization employs controls at various levels throughout the entity at the business process, entity, and technology levels. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has designed application-enforced segregation of duties to define what privileges are assigned to users within applications. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts: element_322_fe8862cadb3bcc98567263dffd3e120b-Access Control Standard.pdf element_322_fe8862cadb3bcc98567263dffd3e120b-ISO 27001 Compliance Matrix.pdf element_322_01d7b39b0ab73572946a70b170e15e3c-Review.pdf element_322_dd593a8ead42313546329e148161da25-CAB1.pdf				
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**1.** Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls. **2.** Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing. **3.** Establishes Relevant Security Management Process Controls	As part of the annual business planning, strategic technology risks affecting the organization and recommended courses of action are identified and discussed. As evidenced by the annual risk assessment report and Organizational Assessment and Monitroing Standard. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	No relevant exceptions noted.

		Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats. **4.** Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	interviews with key personnel. Management has developed a list of control activities to manage the technology infrastructure risks identified during the annual risk assessment process. As evidenced by the annual risk assessment report and external vulnerability assessments. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management has developed a list of control activities to manage the security access management risks identified during the annual risk assessment process. As evidenced by the annual risk assessment report and access control assessment documentation.	

			The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization employs tailored acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts: element_337_858ba40cf1d3ec08d6c198c8ed49f8ab-Organizational Assessment & Monitoring Standard.pdf element_337_858ba40cf1d3ec08d6c198c8ed49f8ab-ISO 27001 Compliance Matrix.pdf element_337_858ba40cf1d3ec08d6c198c8ed49f8ab-Risk Assessment & Monitoring Standard.pdf element_337_f2e0f5359ae701280d15c223da297188-CAB1.pdf				
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**1.** Establishes Policies and Procedures to Support Deployment of Management 's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions. **2.** Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside. **3.** Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as	The organization has established an Organizational Assessment and Monitoring Standard to address controls over significant aspects of operations. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established an Organizational Assessment and Monitoring Standard to assign reponsibility for establishing, maintaining, and enforcing the overall	No relevant exceptions noted.

		defined by the policies and procedures. **4.** Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities. **5.** Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus. **6.** Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	security policies and procedures. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Senior Management is responsible for the internal audit program and performs internal control testing to ensure personnel perform control activities in a timely manner. Any deficiencies identified are reported to Senior Leadership. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Assessment reports are reviewed at Senior Managements meetings and require the development of corrective	

			action plans for control weaknesses. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has written job descriptions specifying the responsibilities and the academic and professional requirements for key job positions. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization's policy and procedure are reviewed annually by the Senior Management for consistency with the organization's risk mitigation strategy and updated as	

			necessary for changes in the strategy. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

Artifacts:

element_348_9c495d7296d932c5fde054c98b504a54-ISO 27001 Compliance Matrix.pdf
element_348_9c495d7296d932c5fde054c98b504a54-Auditing Standard.pdf
element_348_9c495d7296d932c5fde054c98b504a54-Developer - Integration Job Description.pdf
element_348_9c495d7296d932c5fde054c98b504a54-Developer - Platform Job Description.pdf
element_348_9c495d7296d932c5fde054c98b504a54-Policy Acknowledgement Form.pdf
element_348_9c495d7296d932c5fde054c98b504a54-Information Security Program Charter.pdf
element_348_9961157df6faa5ea930bb78d02eb1bc5-Safari - Mar 28, 2019 at 12_42 PM 2 (1).pdf
element_348_9961157df6faa5ea930bb78d02eb1bc5-Safari - Mar 28, 2019 at 12_42 PM 3 (2).pdf
element_348_9961157df6faa5ea930bb78d02eb1bc5-Safari - Mar 28, 2019 at 12_42 PM (2).pdf
element_348_b6e688cbe8277b8564cb46ab458d02aa-Review.pdf
element_348_b88b41753aff385b45d0dd2db55ccace-CAB1.pdf

	Logical and Physical Access Controls			
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**1.** Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets. **2.** Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets. **3.** Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely. **4.** Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	The organization classifies and maintains an inventory of in-scope information assets through automated mechanisms. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Multifactor authentication is required to access the production information assets. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	No relevant exceptions noted.

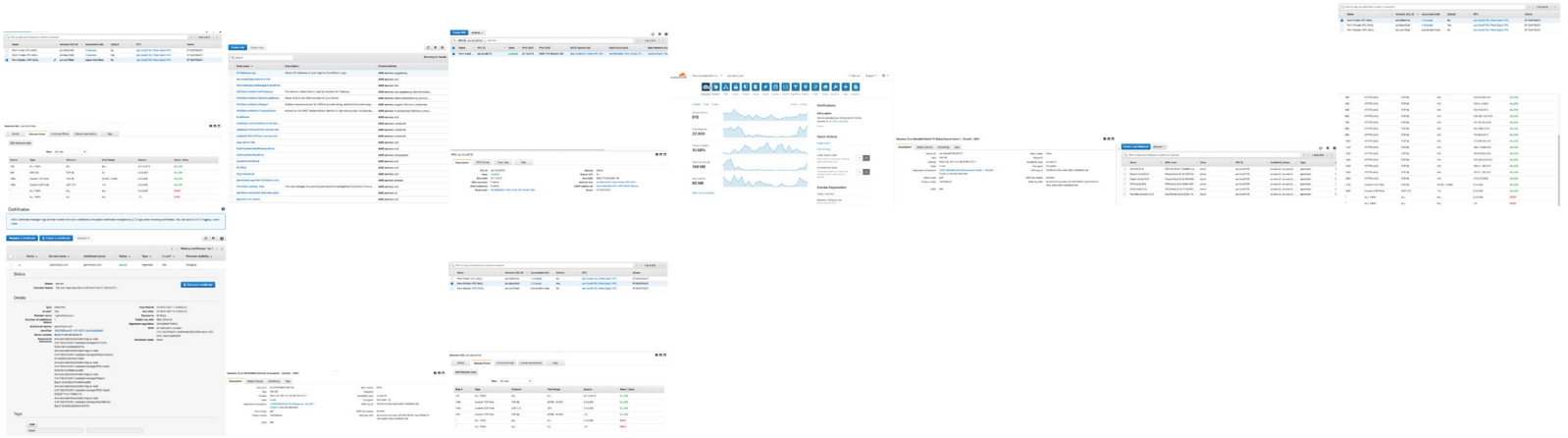
		5. Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed. **6.** Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets. **7.** Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software. **8.** Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point.	In-scope system components require unique username and passwords prior to authenticating users. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization's production network is segmented logically to isolate unrelated portions of the network. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are	

		Credentials are removed, and access is disabled when access is no longer required, or the infrastructure and software are no longer in use. **9.** Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk. **10.** Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.	created to remove access as necessary in a timely manner. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. SSL certificates are used for verification, issuance, signature algorithm, and validity date. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Passwords for in-scope system components are configured according to the	

			organization's policy, which requires eight-character minimum and 90-day password changes; complexity enabled; and enforces an inactivity lockout. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The Configuration Management Standard requires that all system changes undergo formal documentation, review, and authorization. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

			Databases housing sensitive customer data are encrypted at rest. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Encryption keys used by integrated services are encrypted themselves with a unique master key. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts:

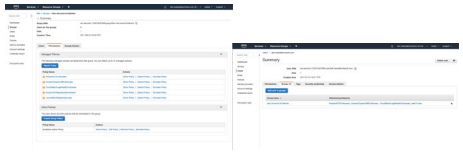


element_365_00babccb38287d482fed71fcae8a8543-scribsoft responses.docx
element_365_00babccb38287d482fed71fcae8a8543-permitium responses.docx
element_365_00babccb38287d482fed71fcae8a8543-Termination Checklist Standard (2).pdf
element_365_00babccb38287d482fed71fcae8a8543-scribbles_employee_exit_interview (1) (1).pdf
element_365_00babccb38287d482fed71fcae8a8543-Miranda_Maner_Access_Form (1).pdf
element_365_00babccb38287d482fed71fcae8a8543-Universal Access Control Form Standard (1).pdf

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**1.** Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian. **2.** Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access. **3.** Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.	Access to in-scope system components requires an authorization based on job description during onboarding before access is provisioned. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. A termination checklist is completed and access is revoked for employees as part of the termination process. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Management performs a quarterly access review for the in-scope system	No relevant exceptions noted.

			components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	
Artifacts: element_388_a4f9068a241e419747a9611ebb28dd40-Miranda_Maner_Access_Form.pdf element_388_a4f9068a241e419747a9611ebb28dd40-scribbles_employee_exit_interview (1).pdf element_388_a4f9068a241e419747a9611ebb28dd40-Termination Checklist Standard (1).pdf element_388_5c36f78848083285ede004e2c251edb3-CAB1 (1).pdf				
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and	**1.** Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	Asset owners periodically review access to ensure continued appropriateness. Requests to create or modify access are processed through an access control form which must be formally	No relevant exceptions noted.

	other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**2.** Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access. **3.** Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.	approved by the Asset owner. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. A termination checklist is completed and access is revoked for employees as part of the termination process. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and privileges into roles.	

			The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	
Artifacts:  element_397_5deb014a9d687a3d9c8a320557535960-Miranda_Maner_Access_Form.pdf element_397_5deb014a9d687a3d9c8a320557535960-Termination Checklist Standard.pdf element_397_5deb014a9d687a3d9c8a320557535960-Universal Access Control Form Standard.pdf				
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities,	**1.** Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.	Noted that the organization hosts information system infrastructure on Amazon Web Services and that Amazon is responsible for design and operation of physical access control processess. Per Inspection of the Amazon Web Services	No relevant exceptions noted.

	back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**2.** Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access. **3.** Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	System SOC 2 report dated November 14, 2018, further noted that physical access controls operated effectively during the audit period. Please refer to the Amazon Web Services System SOC 2 report. Noted that the organization hosts information system infrastructure on Amazon Web Services and that Amazon is responsible for design and operation of physical access control processess. Per Inspection of the Amazon Web Services System SOC 2 report dated November 14, 2018, further noted that physical access controls operated effectively during the audit period. Please refer to the Amazon Web Services System SOC 2 report. Noted that the organization hosts information system infrastructure on Amazon Web Services and that Amazon is responsible for design and operation of physical access control	

			processess. Per Inspection of the Amazon Web Services System SOC 2 report dated November 14, 2018, further noted that physical access controls operated effectively during the audit period. Please refer to the Amazon Web Services System SOC 2 report.	
Artifacts: element_406_778e5ec6bbba52783f4298bd289bfad3-AWS-SOC2-Report_Apr1-Sep30_2018.pdf				
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been	**1.** Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable. **2.** Removes Data and Software From Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity	The organization has established policies and proceures to identify data and software stored on equipment to be disposed and to render such data and software unreadable. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	No relevant exceptions noted.

	diminished and is no longer required to meet the entity's objectives.	and to render such data and software unreadable.	interviews with the organization's staff. Noted that the organization hosts information system infrastructure on Amazon Web Services and that Amazon is responsible for design and operation of physical access control processess. Per Inspection of the Amazon Web Services System SOC 2 report dated November 14, 2018, further noted that physical access controls operated effectively during the audit period. Please refer to the Amazon Web Services System SOC 2 report. The organizaiton has established procedures to remove data and software stored on equipment to be removed from the control of the entity and to render such data and software unreadable. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical	

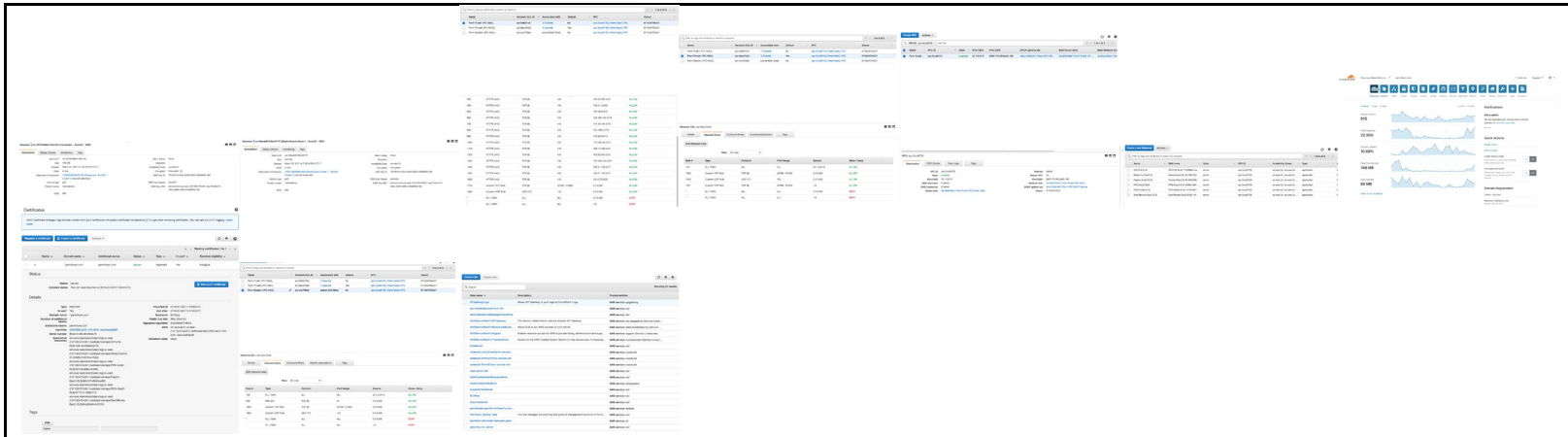
			testing, and technical interviews with the organization's staff. Noted that the organization hosts information system infrastructure on Amazon Web Services and that Amazon is responsible for design and operation of physical access control processess. Per Inspection of the Amazon Web Services System SOC 2 report dated November 14, 2018, further noted that physical access controls operated effectively during the audit period. Please refer to the Amazon Web Services System SOC 2 report.	

Artifacts:

element_415_f66f5e26cf770a5ff114ca000c019ef6-AWS-SOC2-Report_Apr1-Sep30_2018.pdf
element_415_97255def93c823e133e2b91fb48eeed6-scribbles-asset-ic-information-labeling-standard (1).pdf
element_415_97255def93c823e133e2b91fb48eeed6-scribbles-media-sanitation-destruction-policy (1).pdf
element_415_97255def93c823e133e2b91fb48eeed6-scribbles-asset-ic-information-classification-standard.pdf
element_415_97255def93c823e133e2b91fb48eeed6-scribbles-asset-ic-asset-identification-and-classification-standard.pdf

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**1.** Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted. **2.** Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries. **3.** Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries. **4.** Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	System firewalls are configured to limit unnecessary ports, protocols, and services. The only ports open into the environment are defined. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information over public networks. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Multifactor authentication is required to access the	No relevant exceptions noted.

			system boundary. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Boundary protection systems are implemented to protect external access points from attempts and unauthorized access. All external access attempts are logged and monitored. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	
Artifacts:				

				
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the	**1.** Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information. **2.** Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points. **3.** Protects Removal Media—Encryption technologies and physical asset protections are used for removable	The information system restricts the ability of users to transmit, move, or remove system information to other information systems or networks. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Encryption technologies or secured communication channels and protocols are	No relevant exceptions noted.

	entity's objectives.	media (such as USB drives and back-up tapes), as appropriate. **4.** Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones and tablets) that serve as information assets.	used to protect transmission of data and other communications beyond connectivity access points. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Removable media is not permitted or used for in-scope systems. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. There are no mobile devices that serve as information assets. The assessor verified the system design, policy requirements, and technical enforcement through visual	

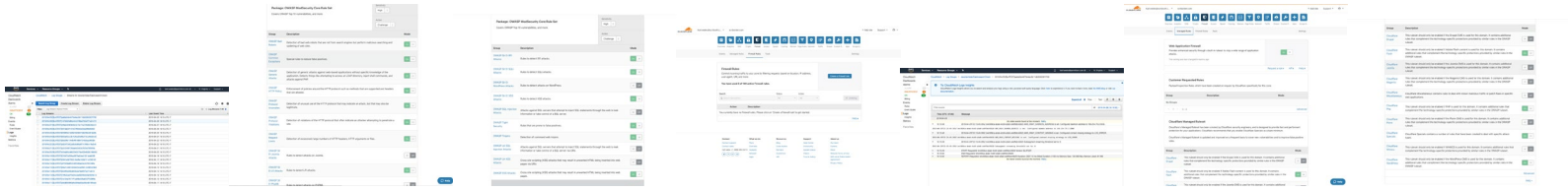
			inspections, technical testing, and technical interviews with the organization's staff.	
Artifacts: 				
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious	**1.** Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals. **2.** Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the rules of behavior and acceptable use policies.	No relevant exceptions noted.

	software to meet the entity's objectives.	indicative of unauthorized or malicious software. **3.** Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software. **4.** Uses Antivirus and Anti-Malware Software—Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware. **5.** Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.	The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organizations has established processes to review logs and generate alerts for system adminsitrators to detect unauthorized changes to software or configurations. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security	

			and availability requirements. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Anti-malware technology is deployed for environments commonly susceptible to malicious attacks. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Logging and monitoring tools are used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource	

			utilization, and to detect unusual system activity or service requests. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts:



	System Operations

CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**1.** Uses Defined Configuration Standards—Management has defined configuration standards. **2.** Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives. **3.** Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files. **4.** Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components. **5.** Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	The organization has a Configuration Management Standard which establishes requirements for maintaining baseline configurations of information assets. The Configuration Management Standard is reviewed on at least an annual basis. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Infrastructure monitoring tools are utilized to monitor infrastructure availability and performance and generates alerts when specific predefined thresholds are met. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	No relevant exceptions noted.

			interviews with the organization's staff. The organization utilizes resource monitoring tools that notify administrators of changes to production systems. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Automated mechanisms are used to continuously monitor production resources for the addition of unauthorized components/devices. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Internal and external network vulnerability scans are performed at least annually. A remediation	

			plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	
Artifacts: element_458_8595a02c9726b29362b5eb8ebddcb9a7-penn-testing-03202019.pdf element_458_dee684c33ba4b09681d590e11508b404-Safari - Apr 25, 2019 at 2_19 PM.pdf element_458_dee684c33ba4b09681d590e11508b404-Safari - Apr 25, 2019 at 2_37 PM.pdf element_458_830e17c39e525aa575252a5d23732d74-Configuration Management Standard.pdf				
CC7.2	The entity monitors system components and the operation of those components for	**1.** Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual	The organization has established policies for monitoring information assets, system auditing, vulnerability assessment, and threat assessment to identify anomalies in operation or unusual activity on systems.	No relevant exceptions noted.

	anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities. **2.** Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software. **3.** Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events. **4.** Monitors Detection Tools for Effective Operation—Management has	As evidenced by the Vulnerability Assessment and Monitoring Standard, Vulnerability Management Standard, Threat Monitoring Standard, and Auditing Standard. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization has implemented boundary protection mechanisms to provide continuous monitoring of the network to detect threats and prevent unauthorized acess. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

		implemented processes to monitor the effectiveness of detection tools.	The organization has established standards for monitoring information assets,vulnerability assessment, and threat assessment to filter, summarize, and analyze anomalies to identify security events. As evidenced by the Vulnerability Assessment and Monitoring Standard, Vulnerability Management Standard, Threat Monitoring Standard, and Auditing Standard. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization has established standards for monitoring information assets, system, vulnerability assessment, and threat assessment to filter, summarize, and analyze anomalies to identify security events. As evidenced by the	

			Vulnerability Assessment and Monitoring Standard, Vulnerability Management Standard, Threat Monitoring Standard, and Auditing Standard. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts:

element_472_05f6d7b586738b3769373c6f970e5979-Change Advisory Board Charter.docx
element_472_05f6d7b586738b3769373c6f970e5979-scribsoft responses.docx
element_472_03fc9c92534f680bbf2d00b942ce125a-Vulnerability Management Standard.pdf
element_472_03fc9c92534f680bbf2d00b942ce125a-Vulnerability Assessment & Management Standard.pdf
element_472_03fc9c92534f680bbf2d00b942ce125a-Threat Assessment & Monitoring Standard.pdf
element_472_03fc9c92534f680bbf2d00b942ce125a-Threat Monitoring Standard.pdf
element_472_03fc9c92534f680bbf2d00b942ce125a-Integrity Protection Standard.pdf

CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**1.** Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis. **2.** Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary. **3.** Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact. **4.** Assesses the Impact on Personal Information—Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations. **5.** Determines Personal Information Used or Disclosed—When an unauthorized use or disclosure of personal	The organization has developed security incident response policies and procedures that are communicated to authorized users. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	No relevant exceptions noted.

		information has occurred, the affected information is identified.	The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. A formal Incident Response Plan is documented and communicated to authorized users and includes detection and anlaysis procedures to assess the potential impact of an incident. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Detected security events are evaluated to determine whether they could or did result in an unauthorized disclosure or use of personal information and whether there has been a failure to	

			comply with applicable laws or regulations. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. If an unauthorized use or disclosure of personal information has been identified, the affected information is identified in incident reports and documentation. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts: element_483_db90a655bc3708d71730a68d35414a4a-Information Security Program Charter (4).pdf element_483_db90a655bc3708d71730a68d35414a4a-Threat Monitoring Standard (1).pdf element_483_db90a655bc3708d71730a68d35414a4a-Risk Assessment & Monitoring Standard (1).pdf element_483_db90a655bc3708d71730a68d35414a4a-Safari - Apr 23, 2019 at 10_58 AM.pdf element_483_db90a655bc3708d71730a68d35414a4a-Information Security Incident Response Plan (2).pdf				
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**1.** Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary. **2.** Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives. **3.** Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents. **4.** Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident. The assessor verified the system design, policy	No relevant exceptions noted.

		access, and other remediation actions. **5.** Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives. **6.** Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives. **7.** Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach. **8.** Remediates Identified Vulnerabilities—Identified vulnerabilities are	requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Incident response policies and procedures to determine that procedures are in place to mitigate the effects of ongoing security incidents. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions. The assessor verified the system design, policy requirements, and technical enforcement through visual	

		remediated through the development and execution of remediation activities. **9.** Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program. **10.** Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis. **11.** Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes. **12.** Communicates Unauthorized Use and Disclosure—Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required. **13.** Application of Sanctions—The conduct of individuals and	inspections, technical testing, and technical interviews with the organization's staff. Recovery procedures are in place to restore data and business operations to an interim state that permits the achievement of organization's objectives. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	

		organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.	interviews with the organization's staff. The organization has established containment strategies in the Incident Response Plan and procedures. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Internal and external network vulnerability scans are performed at least annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	

			interviews with the organization's staff. Incident reponse policies and procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization incorporates lessons learned from ongoing incident response activities into incident response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel.	

			The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization analyzes the root cause and frequency of incidents related to security, availability, processing integrity, confidentiality, and privacy to identify the need for system changes. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization has established an Incident Response Plan to respond to events that result in unauthorized use or disclosure of personal information and ensure it is communicated to the	

			data subjects, legal and regulatory authorities, and others as required. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Conduct of individuals and organizations operating under the authority of the organization and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, are sanctioned in accordance with entity policies and legal and regulatory requirements. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts: element_496_83ea18486d2abee2711f8957162de665-Review.pdf element_496_83ea18486d2abee2711f8957162de665-Information Security Program Charter (4).pdf element_496_83ea18486d2abee2711f8957162de665-Safari - Apr 23, 2019 at 10_58 AM.pdf element_496_83ea18486d2abee2711f8957162de665-Threat Monitoring Standard (1).pdf element_496_83ea18486d2abee2711f8957162de665-Risk Assessment & Monitoring Standard (1).pdf element_496_83ea18486d2abee2711f8957162de665-ReviewF881A.pdf element_496_83ea18486d2abee2711f8957162de665-Information Security Incident Response Plan (2).pdf element_496_77deaf92387fea27962d7924a145d190-CAB1.pdf				
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	**1.** Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed. **2.** Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).	The organization has established a Configuration Management Standard to manange changes including patches/updates and configuration is controlled through virtual instance testing and have a rollback capability. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	No relevant exceptions noted.

		3. Determines Root Cause of the Event—The root cause of the event is determined. **4.** Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis. **5.** Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved. **6.** Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	interviews with the organization's staff. All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Personnel responsible for security incident tickets follow a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next, the root cause is determined, and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines	

			detailed in the incident response procedures. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. An assessment of the incident response to better handle future incidents is performed through analysis after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization incorporates lessons learned from ongoing incident response activities into incident	

			response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Annual testing of the incident response plan is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned from testing are used to implement changes to reflect effective procedures when handling incidents. The assessor verified the system design, policy requirements, and technical	

			enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts:

element_526_b60406fb15174203d354d6aab169d51e-CAB1.pdf
element_526_b85dd969cb4f7bd2db8ef2768bdfa418-Vulnerability Management Standard.pdf
element_526_b85dd969cb4f7bd2db8ef2768bdfa418-Vulnerability Assessment & Management Standard.pdf
element_526_b85dd969cb4f7bd2db8ef2768bdfa418-Threat Assessment & Monitoring Standard.pdf
element_526_b85dd969cb4f7bd2db8ef2768bdfa418-Threat Monitoring Standard.pdf
element_526_b85dd969cb4f7bd2db8ef2768bdfa418-Security Incident Report.pdf
element_526_b85dd969cb4f7bd2db8ef2768bdfa418-Information Security Incident Response Plan.pdf

	Change Management			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves,	**1.** Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software and procedures) is used to	The organization has established system development lifecycle policies that define a process for managing changes throughout the product lifecycle. Integral to this policy are change	No relevant exceptions noted.

	and implements changes to infrastructure, data, software, and procedures to meet its objectives.	support system availability and processing integrity. **2.** Authorizes Changes—A process is in place to authorize system changes prior to development. **3.** Designs and Develops Changes—A process is in place to design and develop system changes. **4.** Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities. **5.** Tracks System Changes—A process is in place to track system changes prior to implementation. **6.** Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software. **7.** Tests System Changes—A process is in place to test system changes prior to implementation. **8.** Approves System Changes—A process is in place to approve system changes prior to implementation.	management steps addressing the design aspects, development requirements, acquisition requirements, and business objectives. Change management controls include all requirements for testing, approvals, and implementation aspects of the change management process. As evidenced by the Software Development Life Cycle Standard, Software Development Communication Cycle standard, Change Advisory Board Charter, and the Configuration Management Standard. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization's software and infrastructure change management process	

		9. Deploys System Changes—A process is in place to implement system changes. **10.** Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle. **11.** Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification. **12.** Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained. **13.** Provides for Changes Necessary in Emergency Situations —A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations (that is, changes that need	require that change requests are: • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements. The assessor verified the system design, policy requirements, and technical	

		to be implemented in an urgent timeframe). **14.** Protects Confidential Information—The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality. **15.** Protects Personal Information—The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.	enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization requires all system changes to be documented to support ongoing maintenance of the system and to support system users in performing their responsibilities. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization requires all system changes to be tracked prior to implementation. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	

			interviews with the organization's staff. Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed when required due to reviews and system changes. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation. The assessor verified the system design, policy requirements, and technical enforcement through visual	

			inspections, technical testing, and technical interviews with the organization's staff. The organization maintains a formally documented change management process that is reviewed and approved by appropriate personnel prior to implementation. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing and technical interviews with the organization's staff. The organization maintains a formally documented change management process and procedure to implement system changes. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical	

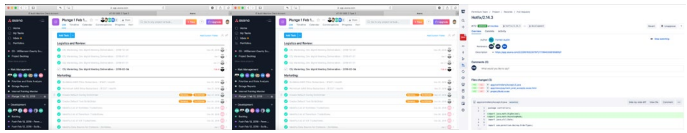
			interviews with the organization's staff. The organization maintains a formally documented change management process to identify and evaluate system changes to determine whether they meet design requirements and system objectives. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. The organization contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan of action for each recommendation and follows up on open recommendations.	

			The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated when required due to reviews and system changes , and anytime integral system components are added. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Emergency changes follow the standard change management process but at	

			an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address confidentiality requirements. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff. Change management procedures (including	

			emergency procedures) are in place to govern the modification and maintenance of production systems and address privacy requirements. The assessor verified the system design, policy requirements, and technical enforcement through visual inspections, technical testing, and technical interviews with the organization's staff.	

Artifacts:



element_542_cbda52914c58aa11e234c86df6d98bc3-Agenda.pdf
element_542_b382136c88730cd9d14cdca4810ee609-Safari - Apr 25, 2019 at 2_19 PM.pdf
element_542_b382136c88730cd9d14cdca4810ee609-Safari - Apr 25, 2019 at 2_37 PM.pdf
element_542_77fa5398dfeaf86622177ba9aaee2312-Software Development Communication Cycle Standard.pdf element_542_77fa5398dfeaf86622177ba9aaee2312-Software Development Life Cycle Standard.pdf element_542_77fa5398dfeaf86622177ba9aaee2312-Change Advisory Board Charter.pdf

element_542_77fa5398dfeaf86622177ba9aaee2312-Configuration Management Standard.pdf element_542_77fa5398dfeaf86622177ba9aaee2312-Fix issue causing certain error messages not to properly display on accept js p… - Asana.pdf				
	Risk Mitigation			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**1.** Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts. **2.** Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed. As evidenced by the annual risk assessment report. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	No relevant exceptions noted.

			The risk management program includes the use of insurance to minimize the financial impact of any loss events. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	
Artifacts: element_579_820b0be27c1cf6af3774b5b629a3cf73-COI - Mecklenburg Co Sheriff NC.pdf element_579_0ad8df381394876d50b9b2924eaaaafc-CAB1.pdf				
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	**1.** Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	The organization has established requirements for vendor and business partner engagements that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels. The	No relevant exceptions noted.

		2. Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives. **3.** Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners. **4.** Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners. **5.** Establishes Exception Handling Procedures from Vendors and Business Partners —The entity establishes exception handling procedures for service or product issues related to vendors and business partners. **6.** Assesses Vendor and Business Partner Performance—The entity periodically	assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established an Organizational Assessment and Monitoring Standard to assess vendors and business partners on a periodic basis. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established an Organizational Assessment and Monitoring Standard to assign responsibility and accountability for managing risks assocaited with vendors and business partners.	

		assesses the performance of vendors and business partners. **7.** Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships. **8.** Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships. **9.** Obtains Confidentiality Commitments from Vendors and Business Partners—The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information. **10.** Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors	The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has documented and communicated security policies that define the information security rules and requirements for the service environment related	

		and business partners with the entity's confidentiality commitments and requirements. **11.** Obtains Privacy Commitments from Vendors and Business Partners—The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information. **12.** Assesses Compliance with Privacy Commitments of Vendors and Business Partners— On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.	to vendors and business partners. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. Inspected risk assessment documentation to determine that a risk assessment was performed within the past year. Inspected security policies to determine entity has established defined roles and responsibilities to oversee implementation of information security policies. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established exception	

			handling procedures for service or product issues related to vendors and business partners. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization has established policies and procedures for terminating vendor and business partner relationships. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization obtains and periodically reviews confidentiality commitments that are consistent with the organization's confidentiality	

			commitments and requirements from vendors and business partners who have access to confidential information. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. The organization assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements periodically and when external assessment reports for the vendor or business partner are made available. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel.	

			The organization obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and interviews with key personnel. On a periodic and as-needed basis, the organization assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary. The assessor verified compliance with this control objective through the examination of documentation and policies, direct observation, and	

			interviews with key personnel.	

Artifacts:

element_586_681eb22438dbca5227277b28329c749f-Vulnerability Management Standard.pdf element_586_681eb22438dbca5227277b28329c749f-Vulnerability Assessment & Management Standard.pdf element_586_681eb22438dbca5227277b28329c749f-Threat Monitoring Standard.pdf element_586_681eb22438dbca5227277b28329c749f-Organizational Assessment & Monitoring Standard.pdf element_586_681eb22438dbca5227277b28329c749f-Organizational Assessment & Monitoring StandardBAA93.pdf element_586_681eb22438dbca5227277b28329c749f-Organizational Assessment & Monitoring Standard42E6A.pdf element_586_681eb22438dbca5227277b28329c749f-Service Level Agreement Standard.pdf element_586_a95d182a55171b782db1ee78394a3f4d-COI - Mecklenburg Co Sheriff NC.pdf element_586_8d9b1c45f25acba033f90240449629ba-AWS-SOC2-Report_Apr1-Sep30_2018.pdf

	Additional Criteria for Availability			
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system	**1.** Measures Current Usage—The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.		Not in scope.

	components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**2.** Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity. **3.** Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.		
Artifacts:				
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections,	**1.** Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water. **2.** Designs Detection Measures—Detection measures are implemented		Not in scope.

	software, data back-up processes, and recovery infrastructure to meet its objectives.	to identify anomalies that could result from environmental threat events. **3.** Implements and Maintains Environmental Protection Mechanisms— Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events. **4.** Implements Alerts to Analyze Anomalies—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events. **5.** Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem). **6.** Communicates and Reviews Detected Environmental Threat Events—Detected environmental threat events are communicated to and reviewed by the individuals		

		responsible for the management of the system, and actions are taken, if necessary. **7.** Determines Data Requiring Backup—Data is evaluated to determine whether backup is required. **8.** Performs Data Backup—Procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur. **9.** Addresses Offsite Storage—Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level. **10.** Implements Alternate Processing Infrastructure—Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.		
Artifacts:				

A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**1.** Implements Business Continuity Plan Testing—Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results. **2.** Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.		Not in scope.
Artifacts:				
	Additional Criteria for Confidentiality			

C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	**1.** Identifies Confidential information—Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained. **2.** Protects Confidential Information from Destruction—Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.		Not in scope.
Artifacts:				
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	**1.** Identifies Confidential Information for Destruction—Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached. **2.** Destroys Confidential Information—Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.		Not in scope.

Artifacts:				
	Additional Criteria for Processing Integrity			
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the	**1.** Identifies Information Specifications—The entity identifies information specifications required to support the use of products and services. **2.** Defines Data Necessary to Support a Product or Service—When data is provided as part of a service or product or as part of a reporting obligation related to a product or service: **a.** The definition of the data is available to the users of the data **b.** The definition of the data includes the following information: **c.** The population of events or instances included in the data		Not in scope.

	use of products and services.	**d.** The nature of each element (for example, field) of the data (that is, the event or instance to which the data element relates, for example, transaction price of a sale of Permitium, LLC Corporation stock for the last trade in that stock on a given day) **e.** Source(s) of the data **f.** The unit(s) of measurement of data elements (for example, fields) **g.** The accuracy/correctness/precision of measurement **h.** The uncertainty or confidence interval inherent in each data element and in the population of those elements **i.** The date the data was observed or the period of time during which the events relevant to the data occurred **j.** The factors in addition to the date and period of time used to determine the inclusion and		

		exclusion of items in the data elements and population **k.** The definition is complete and accurate. **3.** The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (meta-data) that has not been included within the data.		
Artifacts:				
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to	**1.** Defines Characteristics of Processing Inputs—The characteristics of processing inputs that are necessary to meet requirements are defined. **2.** Evaluates Processing Inputs—Processing inputs are evaluated for compliance with defined input requirements. **3.** Creates and Maintains Records of System Inputs—Records of system input activities are created and		Not in scope.

	meet the entity's objectives.	maintained completely and accurately in a timely manner.		
Artifacts:				
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	**1.** Defines Processing Specifications—The processing specifications that are necessary to meet product or service requirements are defined. **2.** Defines Processing Activities—Processing activities are defined to result in products or services that meet specifications. **3.** Detects and Corrects Production Errors—Errors in the production process are detected and corrected in a timely manner. **4.** Records System Processing Activities—System processing activities are recorded completely and accurately in a timely manner. **5.** Processes Inputs—Inputs are processed completely, accurately, and timely as authorized in		Not in scope.

		accordance with defined processing activities.		
Artifacts:				
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	**1.** Protects Output—Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting specifications. **2.** Distributes Output Only to Intended Parties—Output is distributed or made available only to intended parties. **3.** Distributes Output Completely and Accurately—Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output. **4.** Creates and Maintains Records of System Output Activities—Records of system output activities are created and maintained completely and accurately in a timely manner.		Not in scope.

Artifacts:				
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	**1.** Protects Stored Items—Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications. **2.** Archives and Protects System Records—System records are archived, and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used. **3.** Stores Data Completely and Accurately—Procedures are in place to provide for the complete, accurate, and timely storage of data. **4.** Creates and Maintains Records of System Storage Activities—Records of system storage activities are created and maintained completely and accurately in a timely manner.		Not in scope.

Artifacts:				
	Additional Criteria for Privacy			
P1.0	**Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy**			
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a	**1.** Communicates to Data Subjects—Notice is provided to data subjects regarding the following: **a.** Purpose for collecting personal information **b.** Choice and consent **c.** Types of personal information collected **d.** Methods of collection (for example, use of cookies or other tracking techniques) **e.** Use, retention, and disposal **f.** Access		Not in scope.

	timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	**g.** Disclosure to third parties **h.** Security for privacy **i.** Quality, including data subjects' responsibilities for quality **j.** Monitoring and enforcement **2.** If personal information is collected from sources other than the individual, such sources are described in the privacy notice. **3.** Provides Notice to Data Subjects—Notice is provided to data subjects (1) at or before the time personal information is collected or as soon as practical thereafter, (2) at or before the entity changes its privacy notice or as soon as practical thereafter, or (3) before personal information is used for new purposes not previously identified. **4.** Covers Entities and Activities in Notice—An objective description of the entities and activities covered is included in the entity's privacy notice. **5.** Uses Clear and Conspicuous Language—The entity's privacy notice is conspicuous and uses clear language.		

Artifacts:				
P2.0	**Privacy Criteria Related to Choice and Consent**			
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and	**1.** Communicates to Data Subjects—Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise. **2.** Communicates Consequences of Denying or Withdrawing Consent—When personal information is collected, data subjects are informed of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.		Not in scope.

	disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	**3.** Obtains Implicit or Explicit Consent—Implicit or explicit consent is obtained from data subjects at or before the time personal information is collected or soon thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented. **4.** Documents and Obtains Consent for New Purposes and Uses—If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose. **5.** Obtains Explicit Consent for Sensitive Information—Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise. **6.** Obtains Consent for Data Transfers—Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.		

Artifacts:				
P3.0	**Privacy Criteria Related to Collection**			
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	**1.** Limits the Collection of Personal Information—The collection of personal information is limited to that necessary to meet the entity's objectives. **2.** Collects Information by Fair and Lawful Means—Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information. **3.** Collects Information From Reliable Sources—Management confirms that third parties from whom personal information is collected (that is,		Not in scope.

		sources other than the individual) are reliable sources that collect information fairly and lawfully. **4.** Informs Data Subjects When Additional Information Is Acquired—Data subjects are informed if the entity develops or acquires additional information about them for its use.		
Artifacts:				
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the	**1.** Obtains Explicit Consent for Sensitive Information—Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise. **2.** Documents Explicit Consent to Retain Information–Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.		Not in scope.

	consent prior to the collection of the information to meet the entity's objectives related to privacy.			
Artifacts:				
P4.0	**Privacy Criteria Related to Use, Retention, and Disposal**			
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	**1.** Uses Personal Information for Intended Purposes—Personal information is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained unless a law or regulation specifically requires otherwise.		Not in scope.

Artifacts:				
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	**1.** Retains Personal Information—Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise. **2.** Protects Personal Information—Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.		Not in scope.
Artifacts:				
P4.3	The entity securely disposes of personal information to meet the entity's objectives	**1.** Captures, Identifies, and Flags Requests for Deletion—Requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.		Not in scope.

	related to privacy.	**2.** Disposes of, Destroys, and Redacts Personal Information—Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access. **3.** Destroys Personal Information—Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.		
Artifacts:				
P5.0	**Privacy Criteria Related to Access**			
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for	**1.** Authenticates Data Subjects' Identity—The identity of data subjects who request access to their personal information is authenticated before they are given access to that information. **2.** Permits Data Subjects Access to Their Personal Information—Data subjects are able to determine whether the		Not in scope.

	review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	entity maintains personal information about them and, upon request, may obtain access to their personal information. **3.** Provides Understandable Personal Information Within Reasonable Time—Personal information is provided to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any. **4.** Informs Data Subjects If Access Is Denied—When data subjects are denied access to their personal information, the entity informs them of the denial and the reason for the denial in a timely manner, unless prohibited by law or regulation.		
Artifacts:				

P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's	**1.** Communicates Denial of Access Requests—Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation. **2.** Permits Data Subjects to Update or Correct Personal Information—Data subjects are able to update, or correct personal information held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's personal information consistent with the entity's objective related to privacy. **3.** Communicates Denial of Correction Requests—Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.		Not in scope.

	objectives related to privacy.			
Artifacts:				
P6.0	**Privacy Criteria Related to Disclosure and Notification**			
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives	**1.** Communicates Privacy Policies to Third Parties—Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed. **2.** Discloses Personal Information Only When Appropriate—Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless		Not in scope.

	related to privacy.	a law or regulation specifically requires otherwise. **3.** Discloses Personal Information Only to Appropriate Third Parties—Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements. **4.** Discloses Information to Third Parties for New Purposes and Uses—Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.		
Artifacts:				

P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	**1.** Creates and Retains Record of Authorized Disclosures—The entity creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely.		Not in scope.
Artifacts:				
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures	**1.** Creates and Retains Record of Detected or Reported Unauthorized Disclosures—The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is complete, accurate, and timely.		Not in scope.

	(including breaches) of personal information to meet the entity's objectives related to privacy.			
Artifacts:				
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties'	**1.** Discloses Personal Information Only to Appropriate Third Parties—Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements. **2.** Remediates Misuse of Personal Information by a Third Party —The		Not in scope.

	compliance on a periodic and as-needed basis and takes corrective action, if necessary.	entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.		
Artifacts:				
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such	**1.** Remediates Misuse of Personal Information by a Third Party—The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information. **2.** Reports Actual or Suspected Unauthorized Disclosures—A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.		Not in scope.

	notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.			
Artifacts:				
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's	**1.** Remediates Misuse of Personal Information by a Third Party—The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information. **2.** Provides Notice of Breaches and Incidents—The entity has a process for providing notice of breaches and		Not in scope.

	objectives related to privacy.	incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.		
Artifacts:				
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	**1.** Identifies Types of Personal Information and Handling Process—The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. **2.** Captures, Identifies, and Communicates Requests for Information—Requests for an accounting of personal information held and disclosures of the data subjects' personal information are captured, and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.		Not in scope.

Artifacts:				
P7.0	**Privacy Criteria Related to Quality**			
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	**1.** Ensures Accuracy and Completeness of Personal Information—Personal information is accurate and complete for the purposes for which it is to be used. **2.** Ensures Relevance of Personal Information—Personal information is relevant to the purposes for which it is to be used.		Not in scope.
Artifacts:				

P8.0	Privacy Criteria Related to Monitoring and Enforcement			
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related	**1.** Communicates to Data Subjects—Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes. **2.** Addresses Inquiries, Complaints, and Disputes—A process is in place to address inquiries, complaints, and disputes. **3.** Documents and Communicates Dispute Resolution and Recourse—Each complaint is addressed, and the resolution is documented and communicated to the individual. **4.** Documents and Reports Compliance Review Results—Compliance with objectives related to privacy are reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented. **5.** Documents and Reports Instances of Noncompliance—Instances of noncompliance with objectives		Not in scope.

	to identified deficiencies are made or taken in a timely manner.	related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis. **6.** Performs Ongoing Monitoring—Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.		
Artifacts:				