Appropriate Solutions, Inc. dba
Auric Systems International

Service Organization Controls 2, Type II Report

DESCRIPTION OF SYSTEM AND SUITABILITY OF DESIGN
OF THE
DATA TOKENIZATION SERVICE
RELEVANT TO SECURITY, AVAILABILITY, PROCESSING
INTEGRITY, CONFIDENTIALITY, AND PRIVACY

For the Period From

July 1, 2020 To December 31, 2020

HOOD & STRONG LLP
CERTIFIED PUBLIC ACCOUNTANTS
A Century Strong

Table of Contents

SECTION ONE:

Independent Service Auditors' Report Provided by Hood & Strong LLP

HOOD & STRONG LLP
CERTIFIED PUBLIC ACCOUNTANTS

A Century Strong

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of **Auric Systems International:**

Scope

We have examined Auric Systems International's, a division of Appropriate Solutions, Inc. ("Auric") (the "Company") accompanying description of its data tokenization service platform in Section 3 titled "Description of Auric's Data Tokenization Platform" throughout the period July 1, 2020 through December 31, 2020, (the "description") based on the criteria for a description of a service organization's systems in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report ("AICPA, Description Criteria") ("description criteria")* and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2020 through December 31, 2020, to provide reasonable assurance that Auric's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria") set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria") ("AICPA, Trust Services Criteria").

As indicated in the description in Section Three, Auric uses various service organizations to perform hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Auric, to achieve Auric's service commitments and system requirements based on the applicable trust services criteria. The description presents Auric's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Auric's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Auric, to achieve Auric's service commitments and system requirements based on the applicable trust services criteria. The description presents Auric's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Auric's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls throughout the period July 1, 2020 through December 31, 2020.

Service Organization's Responsibilities

Auric is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Auric's service commitments and system requirements were achieved. In Section Two, Auric has provided the accompanying assertion titled "Auric's Assertion" (assertion) about the description and the suitability of the design of controls stated therein. Auric is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

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

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

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

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

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4, "Trust Services Security Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3 and 4.

Opinion

In our opinion, in all material respects,

a. the description presents Auric's Data Tokenization Platform that was designed and implemented throughout the period July 1, 2020 to December 31, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period July 1, 2020 through December 31, 2020, to provide reasonable assurance that Auric's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Auric's controls throughout that period.

c. the controls stated in the description were suitably designed throughout the period July 1, 2020 through December 31, 2020. to provide reasonable assurance that Auric's service commitments and system requirements would be achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Auric's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Auric, user entities of Auric's Data Tokenization Platform throughout the period July 1, 2020 through December 31, 2020, business partners of Auric subject to risks arising from interactions with the travel and expense management processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Hood & Strong LLP

June 17, 2021
San Francisco, CA

SECTION TWO:

Management of Auric's Assertion Regarding its Data Tokenization Platform throughout the period July 1, 2020 through December 31, 2020

Appropriate Solutions, Inc Assertion

We have prepared the description of the Appropriate Solutions, Inc d/b/a Auric Systems International ("ASI") AuricVault® service entitled, "Appropriate Solutions, Inc. d/b/a Auric Systems International Description of its AuricVault® Service," for processing user entities' transactions throughout the period 1 July 2020 to 31 December 2020 ("description") for user entities of the system during some or all of the period 1 July 2020 to 31 December 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

ASI uses a subservice organization to host and manage the production servers. The description includes only the control objectives and related controls of ASI and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of ASI's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

1. the description fairly presents the AuricVault® service system made available to user entities of the system during some or all of the period 1 July 2020 to 31 December 2020 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

    1. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

        (1) the types of services provided, including, as appropriate, the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

(3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

2. includes relevant details of changes to the service organization's system during the period covered by the description.

3. does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the AuricVault® service system that each individual user entity of the system and its auditor may consider important in its own particular environment.

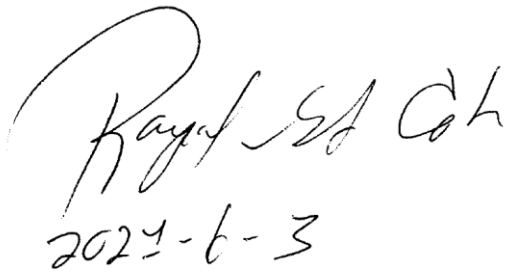
2. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period 1 July 2020 to 31 December 2020 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of ASI's controls throughout the period 1 July 2020 to 31 December 2020. The criteria we used in making this assertion were that:

    1. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

    2. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

    3. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

By:



2021-6-3

Raymond GA Côté, CTO Auric Systems International

SECTION THREE:

Description of Auric's Data Tokenization Service Platform throughout the period July 1, 2020 through December 31, 2020

Management Statement Auric Systems International

OVERVIEW OF OPERATIONS

Company Background

Appropriate Solutions, Inc. (ASI), headquartered in Peterborough, NH USA was founded in 1987 to provide custom software development. In 1994, ASI developed what we believe to be the first Macintosh-based credit card processing software and the first Windows-native credit card processing software (CreditNow!®). From 1994 thru 2006 ASI developed a series of flexible (CN!Express™) and high-volume (Trevance®) payment applications. The Auric Systems International division of Appropriate Solutions, Inc. was created in 2004 to focus exclusively on payment processor and data security solutions.

The PaymentVault™ tokenization application, ASI's first tokenization product, was released as a Windows and Linux application for on-site tokenization in 2007. In 2010, ASI released the PaymentVault™ web service for remote token storage. The PaymentVault™ service was designed to integrate with ASI's payment applications (CN!Express™ and Trevance®).

ASI released a new tokenization service (AuricVault®) in 2013. The AuricVault® service is a general tokenization service designed for tokenizing payments, personally identifiable information, and generally sensitive information. The service provides a back-end Payments Passthrough option to replace ASI's legacy payment applications.

In 2019, ASI released an inbound and outbound proxy tokenization service (AuvProxy) which provides another channel for removing credit card and sensitive data from our client's environments. That year, ASI also introduced the open source Trevance® T4 batch processing application to address custom batch tokenization and payments presentation requirements.

As of 2020, ASI has clients in over 31 countries.

Description of Services Provided

The AuricVault® tokenization service secures vitally sensitive financial and personal data by safely encrypting and storing the data remotely and replacing the original data with a *token*. Tokens are random strings of numbers and letters that have no relationship to the stored data. If someone stole all your tokens, they still would not have any of your sensitive data.

Tokenization provides *data separation*. Data separation ensures that no single entity has all the data at one time. Auric's tokenization solution provides fine-grained permissions for one or more parties to access sensitive tokenized data.

Optional services such as the back-end Payments Passthrough and AuvProxy can convey detokenized (or re-tokenized) data to third parties such as payment processors and order management services.

The AuricVault® service can tokenize:

Financial Data: Credit/Debit Card Account Number, Banking Account Number, Financial Account Number

Identification Data: Biometric Data, Birth Date, Birthplace, Driver's License Information, Email Address, Foreign Passport Visa Information, Mother's Maiden Name, Name and Address, National Insurance Number, Protected Health Information (PHI), Personally Identifiable Information (PII), Passport Number, Social Security Number

Access Data: Access Codes, Passwords, Password Hashes, Security Codes, Fingerprint Templates

The AuricVault® service is hosted within a fully managed Level 1 PCI Compliant environment provided by ASI's hosting partner, Flexential. The AuricVault® service is deployed in geographically redundant facilities in Allentown, PA and Seattle, WA. All data is stored and managed within US borders.

Principal Service Commitments and System Requirements

ASI designs its processes and procedures related to meet its objectives for its AuricVault® services. Those objectives are based on the service commitments that ASI makes to user entities, the laws and regulations that govern the handling and storage of payments and sensitive information including, but not limited to, Level 1 PCI Service Provider, EU-U.S. Privacy Shield, Swiss-U.S. Privacy Shield, General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the New York SHIELD Act, and the financial, operational, and compliance requirements that ASI has established for the services.

Security commitments to user entities are documented and communicated in Services Agreements (SAs) 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 services 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;

- ASI establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ASI's system policies and procedures, system design documentation, and contracts with customers;

- Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained;

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the services.

SYSTEM DESCRIPTION

Infrastructure

The production service infrastructure is hosted and managed by ASI's hosting partner, Flexential. The managed environment consists of:

- Virtual VMWare server instances (via a VMWare ESX privately managed cloud);
- Physical hardware for database servers;
- Physical Cisco firewalls;
- Virtual Load Balancers;
- Red Hat Enterprise Linux versions 6 and 7;
- Intrusion Detection hardware and services;
- Internal and external scanning services for quarterly vulnerability scanning.

A Jump Server installed at the ASI corporate offices provides ASI employees access to the Flexential managed environment. Access to the managed environment requires a VPN connection to the Jump Server and another VPN connection from the Jump Server to the managed environment.

Access to the Jump Server is via a locked door. A sign-in sheet and camera system track access to the physical Jump Server.

Primary Software

The AuricVault® service is developed in house. No third-party payment applications are used. ASI policies maintain a Critical Software List tracking both in house and third-party applications, including databases, web servers, and components used to build the service.

People

ASI utilizes the following functional areas of operations to support the service:

- Executive Management – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner;
- Data Security Officers – responsible for managing and protecting users' information and systems from unauthorized access and use while maintaining integrity and availability;
- IT/Operations – responsible for deploying and maintaining application-level code;
- Development – responsible for specifying, deploying and maintaining infrastructure systems, security, and support for user entities;
- Support –responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, delivering goods, and continued support;
- Marketing/Sales – responsible for marketing and sales functions;
- Human Resources – responsible for managing employee onboarding, termination, payroll, and benefits.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All employees are required to adhere to the ASI policies and procedures that define how services should be delivered. These policies are delivered to all new ASI employees prior to their first day of employment, distributed electronically to all employees when modified, and are acknowledged annually by all employees via a signed acknowledgement form.

Physical Security

General Physical Security

Physical security of the data centers is fully managed by ASI's hosting partner, Flexential.

ASI provides physical security via locked door and cameras to the Jump Server installed at the ASI corporate offices. Camera data is based on activity/motion and is maintained for a minimum of 90 days.

New or Modified Employee Physical Access

All ASI personnel are required to attend yearly security training. Additional training is required for development staff.

Vendor Access

There is no vendor access to the Jump Server installed at the ASI corporate offices. Vendor access to the hosted environment is managed by Flexential.

Customer Access

There is no direct customer access to any of the ASI servers. Customer access is strictly via the API.

Logical Access – Systems Level

New or Modified User Access

Employees have access to ASI systems, applications, and network devices, with access-level restrictions based on specific job functions that the user performs for ASI. New access to the network is initiated by the IT Operations and the Human Resources Department. Access rights are assigned based on the function/role of the new hire.

Access to the Jump Server installed at ASI corporate headquarters is managed by IT creating a new OS-level shell user and installing an SSH certificate for accessing the account. All new user account creation is logged.

Access to the fully managed host environment is managed via the Flexential ticketing system. It requires a new VPN user to be configured as well as OS-level shell user to be created on each server to which the user has new or modified access.

Two factor authentication (password and physical Yubikey) is required for accessing the servers via a VPN.

Terminated Users

The Human Resources Department initiates the employee termination process and instructs IT to revoke the employee's logical access to ASI's network accounts. The Human Resources Department or the employee's supervisor conducts an exit interview with the terminated employee. A termination notification is generated for relevant departments to authorize access revocations from other ASI facilities, network devices, and systems.

User Access Reviews

To help ensure that access to systems, applications, and network devices remains authorized and appropriate over time, management performs user logical access reviews on users who have access to the corporate domain and network devices. This review consists of inspecting the entire user base to verify that no terminated employees have access to the systems and to verify that users' current access rights are still required and appropriate based on job changes or roles they are currently fulfilling within the organization.

Any exceptions identified by management are sent to the system administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

Privileged User Access

Administrative access to network devices is commensurate with job function and is limited to the IT/Operations employees. Administrative access to Linux servers is controlled via Public Key Infrastructure. Keys are granted to a limited number of IT/Operations employees who require access to maintain the servers.

Password Controls and Security

Access to the network within the fully managed hosted environment is restricted by using password protected SSH keys. Network devices are accessed via a VPN.

ASI Customer Portal uses multi-factor authentication and is granted via membership within the ticketing system, which for ASI employees uses authentication via the ASI managed services domain.

Logical Access – Service Level

Logical access to the AuricVault® service API is via credentials provided by ASI. ASI refers to these as Accounts vs. Users.

New Account Credentials

New accounts are initiated by the Sales team and deployed by IT/Operations. During the onboarding process, the Sales team works with the client to define:

- Which client employees are authorized to receive credentials and/or discuss credential modifications;
- The specific credentials configuration, including multiple sub-credentials for data access, segmentation, and retention periods.

The IT/Operations team creates a client-dedicated sandbox testing environment with the requested configuration. Production credentials are generated after the client confirms the sandbox credentials are configured to meet their requirements.

Modified Account Credentials

Clients request modification and additions to the account credentials via ASI support. Support confirms the person making the request is on the authorized list and reviews the change request.

The IT/Operations team makes the requested changes to the sandbox testing environment. Production changes are deployed after the client confirms the sandbox credential changes meet their requirements.

Terminated Accounts

Account termination is originated by the Sales or Support team, either due to a client request or non-payment.

The IT/Operations team deactivates the client's sandbox and production accounts. Automated scripts remove stored client data within 90 days of account termination.

Account Access Reviews

To help ensure that access to systems, applications, and network devices remains authorized and appropriate over time, management performs periodic logical access reviews on accounts with access to the service. This review consists of inspecting all active accounts to verify that no terminated accounts have access to the service.

Any exceptions identified by management are sent to the IT/Operations team for resolution, and the changed access lists are revalidated for completion of the review by management.

Computer Operations

Backups

A fully configured backup of the ASI Jump Server is maintained offline. If the primary Jump Server fails, IT/Operations physically switch the secondary Jump Server onto the network and immediately performs an OS upgrade.

Backups of the hosted environment are managed by the hosting provider.

Network and Internet Availability

Internet accessibility for the hosted environment is managed by the hosting provider.

The Jump Server installed at the ASI corporate offices uses a single public Internet connection. In the case of Internet failure, any urgent service changes or management that needs to occur is done via the hosting provider's ticketing system.

The ASI corporate office network has a cellular fallback capability in case of network connectivity failure.

Service Redundancy

The AuricVault® service is deployed at two geographically distant locations: Allentown, PA and Seattle, WA. Both facilities are maintained live and active. The service uses near real-time multi-master replication between these facilities to ensure current data is maintained at both locations.

Change Control

Changes related to IT infrastructure and applications that are known to, or have the potential to, affect customer services are placed in a scheduled change window. Changes are managed via a ticketing system. Change tickets include:

- The Reason for the change;
- Pre-deployment/sandbox testing, when appropriate;
- Change instructions;
- Testing;
- Backout instructions;
- Management Sign-off.

Data Communications

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

Service Security

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

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with ASI policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by ASI. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Tools requiring installation in the ASI system are implemented through the Change Management process. Scanning is performed with approved scanning templates.

Boundaries of the System

The scope of this report includes the Jump Server installed at ASI corporate headquarters and the fully managed hosting service provided by Flexential.

Corporate Office Address

- 85 Grove Street, Peterborough, NH 03458 USA

Flexential Data Center Addresses

- 744 Roble Road, Allentown, PA 18109 USA
- 2001 6th Avenue, Suite 800, Seattle, WA 98121 USA

This report does not include the Flexential fully managed data centers.

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

Control Environment

Integrity and Ethical Values

Integrity and high ethical standards are qualities essential to the business of ASI and are fundamental standards of behavior for employees. At ASI, the standards of integrity and ethics are demonstrated daily by the personal conduct of management and various controls, including guidelines for handling sensitive information, invention agreements, security policies, and policies stipulating that employees comply with laws, regulations, and corporate policies as a condition of continued employment. In addition, employees are required to acknowledge ASI's stated values and confirm their commitment to upholding these values by performing their responsibilities in a professional and ethical manner. ASI employees are also required to report potential violations or exceptions to these policies that they suspect are being performed by another employee, contractor, or outsider.

Commitment to Competence

The competence of employees is a key element of the control environment. ASI is committed to continuing employee development. This commitment to competence is expressed in the company's personnel policies and related human resource programs. Specific indicators of the commitment to personnel development include recruiting and hiring policies, investment in training and development, and performance monitoring.

ASI's commitment to competence begins with recruiting, which is the joint responsibility of the Human Resources Department and business unit managers. Hiring decisions are based on various factors, including education, prior relative experience, past accomplishments, and evidence of integrity and ethical behavior. In addition, prospective employees will go through reference and background checks before they are hired.

Management's Philosophy and Operating Style

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This includes assignment of authority and responsibility for operating activities and establishment of reporting relationships and authorization protocols. Policies describing appropriate business practices, knowledge, and experience required of key personnel and resources are communicated to employees for carrying out their duties.

Human Resources Policies and Practices

The Human Resources Department communicates to employees expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

ASI's approach to customer service begins with its staff. The organization has attracted and retained a diversified group of experienced professionals. ASI's hiring practices are designed to help ensure that new employees are qualified for their job responsibilities. ASI's hiring policies and guidelines assist in selecting qualified applicants for specific job responsibilities. Employee training is accomplished through supervised on-the-job training, formal in-house training courses, online learning, and external continuing education programs. Department managers are responsible for overseeing the training and development of qualified employees for current and future responsibilities.

Background checks are required for ASI employees, regardless of job function. Applicants first complete an application and an Authorization Check Form (for the background check). The background check is sent to a third-party vendor, which then runs Social Security, criminal (local, national, and federal), and Office of Foreign Assets Control (OFAC) checks; employment history verification; and a motor vehicle check on the individual. Credit checks are conducted for potential employees in certain finance roles.

Background checks are obtained prior to the finalization of an offer. In addition, offer letters mention that offers are pending satisfactory background and reference checks, in case an issue arises in the future.

New hires meet with the Human Resources Department prior to their first day of work to review new hire information, including the *ASI Employee Handbook and Security Policy* which includes a confidentiality policy. The employee cannot report to work until they sign an acknowledgement they received and understand and the *ASI Employee Handbook and Security Policy* and included confidentiality policy.

Performance reviews are conducted on an ad hoc basis. During these reviews, employees are evaluated based upon the responsibilities of their particular job and the values of the company.

Employees are required to meet stated performance and attendance standards and to follow ASI's policies and procedures.

All ASI personnel are required to attend yearly security training. Additional training in operations, security and product development required for development and support roles. Also, periodic security training materials are created by management and distributed to employees.

Risk Assessment Process

ASI has placed into operation a risk assessment process to identify and manage risks that could affect ASI's ability to provide services to its customers. This process requires management to identify significant risks in its areas of responsibility and to implement appropriate measures to address these risks.

Operations management meets periodically to review the status of each area of the company's operations and to assess risks that could affect service delivery to its customers. Also, management holds quarterly meetings to discuss any issues that occurred during the prior weeks and what improvements can be made in operations to help prevent the issue from occurring again. The meeting consists of team leads, managers, and directors from ASI's Operations group. Information accumulated and discussed during these meetings is presented quarterly to the senior and executive management.

ASI created this review to enable ASI to better identify risks, discuss remediation plans for identified risks, and develop action plans to remediate identified risks to help improve ASI's security and availability obligations to its customers. The meetings consist of individuals from various groups throughout the organization, but primarily consist of representatives from Security, Information Technology, Human Resources, Engineering, and Operations.

Integration with Risk Assessment

Along with assessing risks, ASI has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Information and Communications Systems.

ASI has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable ASI to understand business trends in order to maximize efforts and provide optimal services.

Monitoring Controls

Management and supervisory personnel monitor the quality of internal controls as part of their activities.

ASI has implemented a series of management reports and metrics that measure the results of various processes involved in providing services to its customers. Some of the key metrics that the Operations Management Team monitors are as follows:

1. Capacity:

- CPU usage
- Disk usage
- Transaction volume

2. Quality of service:

- Uptime
- Service errors

3. Operations Center:

- Length of time support tickets are open.

The ASI Security, Operations, and Compliance Teams are responsible for implementing procedures and guidelines to identify the risks inherent in ASI's operations. The foundation of the risk management process is management's knowledge of its operations and its close working relationship with its customers. For any risks identified, management is responsible for implementing appropriate measures.

Monitoring of risks is coordinated through various security and operational committees.

On-Going Monitoring

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

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

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures.

Escalation procedures are maintained for responding and notifying management of any identified risks.

Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System Since the Last Review

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

Incident Since the Last Review

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

Criteria Not Applicable to the System

All Common criterion, including Availability, Confidentiality, Security, Privacy, and Processing Integrity are applicable to the ASI Jump Server and AuricVault® Service.

Subservice Organizations

This report does not include the fully managed hosting service provided by Flexential. The Subservice Description of Services Flexential provides includes virtual and physical server hosting, security appliances, network monitoring and security services including intrusion detection, logging, monitoring, and reporting through a staffed security operations center.

Complementary Subservice Organization Controls

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

The following subservice organizations controls should be implemented by Flexential to provide additional assurance that the control objectives described within this report are met:

Subservice Organization – Flexential

Common Criteria

Control Area	Control ID	Control
Logical and Physical Control Access Controls	CC 6.1	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.
	CC 6.2	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.

	CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
	CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
	CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
System Operations	CC 7.1	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.
	CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	CC 7.3	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.
	CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.

Risk Mitigation	CC 9.2	The entity assesses and manages risks associated with vendors and business partners.
Additional	A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

ASI management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service agreements. In addition, ASI performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations;
- Reviewing attestation reports over services provided by vendors and subservice organizations.

COMPLEMENTARY USER ENTITY CONTROLS

ASI's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to ASI's services to be solely achieved by ASI control procedures.

Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ASI.

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

1. User entities are responsible for securely storing and using their Service API credentials.

2. User entities are responsible for timely response to known or suspected incidents reported by ASI personnel.

3. User entities are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.

4. User entities are responsible for providing and maintaining the list of personnel authorized to submit information and/or requests to ASI.

SECTION FOUR:

Information Provided by Independent Service Auditor

Trust Services Security Criteria, Related Controls, and Tests of Controls

1. Purpose and Objectives of the Report

This report on controls placed in operation and tests of operating effectiveness is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of internal controls related to Auric's Data Tokenization Service Platform.

This report, combined with an understanding of the controls, is intended to assist the auditors in planning and performing financial audits of the user organization.

Our documentation of the control structure policies and procedures of TripActions was restricted to the related policies and procedures specified by Auric in Section 3 and were not extended to procedures in effect at customer locations or other control procedures which may not be listed in Section 3. The examination was performed in accordance with AICPA Statement on Auditing Standards No. SSAE-18, Reports on Controls at a Service Organization. It is each customer organization's responsibility to evaluate this information in relation to the internal control structure in place at each client organization in order to assess the total internal control structure. If an effective internal control structure is not in place at client organizations, Auric's control policies and procedures may not compensate for such weaknesses.

Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specific policies and procedures. In addition to descriptions of specific control structure policies and procedures described below, our procedures included descriptions of relevant elements of Auric's control environment including:

- Auric's organizational structure and approach to segregation of duties.
- Management control methods; and,
- Personnel policies and practices

Our review of the control environment included the following procedures to the extent we considered necessary, (a) a review of Auric's organizational structure including the segregation of functional responsibilities, policy statements, transaction processing manuals, personnel policies, procedures and documentation; (b) discussions with management, operations, administrative, and other personnel who are responsible for developing, ensuring adherence to and applying control performance of their assigned duties; and (c) observations of personnel in the performance of their assigned duties.

Control Structure Policies and Procedures

Our tests of the operating effectiveness of control structure policies and procedures included such tests as were considered necessary in the circumstances to evaluate whether those policies and procedures, and the extent of compliance with them, are sufficient to provide reasonable but not absolute assurance that the specified control objectives were achieved during the period from July 1, 2020 through December 31, 2020. Our tests of the operating effectiveness of control structure policies and procedures were designed to cover a representative number of activities throughout the period from July 1, 2020 through December 31, 2020, for each of the control structure policies and procedures listed in Section 3 which are designed to achieve the specified control objectives. In selecting particular tests of the operating effectiveness of control structure policies and procedures, we considered (a) the nature of the policies and procedures being tested; (b) the types and competence of available evidential matter; (c) the control objectives to be achieved; (d) the assessed level of control risk; and (e) the expected efficiency and effectiveness of the test.

2. Description of Tests of Controls and Results Thereof

Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the period from July 1, 2020 through December 31, 2020, for each of the controls listed in Section Three, which are designed to achieve the specific control objectives. In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

Test	Description
Inquiry	*Made inquiries of appropriate personnel responsible for the performance of the control activity and corroborated responses with management.*
Observation	*Observed the application of a specific control activity.*
Inspection	*Inspected documents and reports indicating the performance of the control activity.*

CC 1.0 Common Criteria Related to Control Environment

Control Ref	Control Activity	Test Performed	Test Results
CC 1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC 1.1.1	The company maintains an ethics section within its 'Comprehensive Security Policy', which requires ethical behavior in all activities and also requires proactive notification of any likely unethical behavior to management. Policy also requires management to investigate any notifications of unethical behavior and take appropriate action, up to and including termination if necessary. The 'Comprehensive Security Policy' must be read and acknowledged by all employees annually.	The total population inspected was the company's internal policies and procedures, including a code of ethics.	No exceptions noted.
CC 1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC 1.2.1	The company has delegated development and implementation of security controls to the CTO and CSO. Annually, the CTO and CSO make a presentation to ownership of the current design and performance of company's internal controls for review and oversight. Per policy, any owners who are also responsible for development or performance of internal security controls are required to recuse themselves from oversight and limit their participation to presentation to the remaining owners.	We inspected the company's internal policies and procedures reviewed to confirm annual security controls presentations and the record of the most recent yearly security presentation.	No exceptions noted.

CC 1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC 1.3.1	The company has annual oversight review meetings whereby owners who are also involved in development of the functions reviewed recuse themselves.	We confirmed the existence of an annual oversight review meeting by inspecting all the company's internal policies and procedures.	No exceptions noted.
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC 1.4.1	The company performs reviews of industry salary surveys when needed for staff retention and also provides for regular training and professional development opportunities for staff primarily through its security awareness and secure software development training programs.	We confirmed that an annual salary review is completed by inspecting all the company's internal policies and procedures.	No exceptions noted.
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC 1.5.1	The company designates in policy both primary and secondary Information Security Officers who together are responsible for all security controls and the CEO and CTO are together are designated as responsible and accountable for all other internal controls.	We verified the officers responsible for security controls by inspecting all the company's internal policies and procedures.	No exceptions noted

CC 2.0 Common Criteria Related to Communications and Information

Control Ref	Control Activity	Test Performed	Test Results
CC 2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC 2.1.1	Management reviews documentation provided by third-party providers to ensure providers are in compliance with security and privacy policies.	We inspected compliance documentation inspected by management from 100% of the third-party vendors for the audit period.	No exceptions noted.
CC 2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC 2.2.1	Management publishes and proactively communicates any changes or updates to policies or controls to all staff.	We inspected policy changes made by management to include prompt communication to all staff regarding policy changes.	No exceptions noted.
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC 2.3.1	Management clearly documents service commitments supported by internal controls within the service's Terms of Service.	We inspected the terms of service agreement to verify its existence and details regarding commitments.	No exceptions noted.

CC 3.0 Common Criteria Related to Risk Assessment

Control Ref	Control Activity	Test Performed	Test Results
CC 3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC 3.1.1	Management performs an annual formal risk assessment exercise the results of which are documented and retained.	A population sample of the company's risk assessment was inspected.	No exceptions noted.
CC 3.2 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.			
CC 3.2.1	Management performs an annual formal risk assessment exercise the results of which are documented and retained.	A population sample of the company's risk assessment was inspected.	No exceptions noted.
CC 3.1 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC 3.3.1	All employees undergo a background check as a condition of employment.	We inspected the company's background checks on all new hires.	No exceptions noted.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			

CC 3.4.1	Management examines the impact of any significant service changes that could impact the effectiveness of required controls.	We inspected all changes noted in the risk assessment, which required re-examination.	No exceptions noted.

CC 4.0 Common Criteria Related to Monitoring Activities

Control Ref	Control Activity	Test Performed	Test Results
CC 4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC 4.1.1	Management performs quarterly compliance reviews to confirm and internally attest that controls are still operating effectively.	We inspected all the quarterly compliance review documentation completed by management.	No exceptions noted.
CC 4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC 4.2.1	Management tracks all control deficiencies within its Jira ticketing implementation with formal owner assignment and management review of remediation.	We inspected the population of all control deficiencies during the audit period.	No exceptions noted.

CC 5.0 Common Criteria Related to Control Activities

Control Ref	Control Activity	Test Performed	Test Results
CC 5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC 5.1.1	Management specifically examines and documents the impact of any risk identified in its annual Risk Assessment for any effect to its internal controls.	We inspected the risk assessment report to confirm it documents the impact of risks identified.	No exceptions noted.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC 5.2.1	A risk control matrix (RCM) has been established to track risks and perform periodic reviews of control effectiveness (risk assessments). For each identified risk scenario, a correlating control or control set has been identified to bring risk down to manageable residual levels.	We inspected the company's risk assessment report and confirmed with management that a periodic review of control effectiveness is performed.	No exceptions noted.
CC 5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC 5.3.1	Management publishes and proactively communicates any changes or updates to policies or controls to all staff.	We inspected policy changes made by management to include prompt communication to all staff regarding policy changes.	No exceptions noted.

CC 5.3.2	Employees are required to complete information security awareness training as part of the onboarding process. An annual refresher is performed for existing employees. Management formally monitors compliance with training requirements.	We inspected the security awareness training documentation that is completed yearly by staff.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls

Control Ref	Control Activity	Test Performed	Test Results
CC 6.1 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.			
CC 6.1.1	Access to all servers is restricted to authorized staff who must be authenticated using two factors (2FA). Specifically, an SSH certificate and YubiKey or equivalent physical security token.	We inspected the company's remote access configuration, which includes an effective two-factor authentication process.	No exceptions noted.
CC 6.1.2	All successful and unsuccessful authentication attempts are logged.	We inspected an annual sampling of the company's logging system, which was tested for authentication logs.	No exceptions noted.
CC 6.1.3	All privileged actions over the sudo command are logged.	We inspected an annual sampling of the company's logging system, which tested the Sudo privileged access logs.	No exceptions noted.
CC 6.1.4	A continuously monitored Intrusion Detection System is in place to monitor for unauthorized access attempts.	We inspected the configuration and monitoring logs for company's intrusion detection system.	No exceptions noted.

CC 6.2 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.			
CC 6.2.1	All access grants and removals are tracked and approved via the company's Jira ticketing system.	We inspected all access grant and removal requests for the audit period.	No exceptions noted.
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC 6.3.1	The service provides for internal access based strictly on job role and job need. User entity access to the service is assigned to user entity staff based on granular access rights including separate access rights which allow some users to create data tokens and other, separately managed access rights for allowance to retrieve of decrypt data tokens.	We inspected all documentation to validate a review of vault client service accounts occurred.	No exceptions noted.
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC 6.4.1	Flexential is responsible for restricting physical access to facilities and protected information assets to authorized personnel.	No population was tested as this was carved out.	N/A
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			

CC 6.5.1	Flexential is responsible for restricting physical access to facilities and protected information assets to authorized personnel.	No population was tested as this was carved out.	N/A
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC 6.6.1	A firewall system including VPNs is in place to filter unauthorized inbound network traffic from the internet.	We inspected the company's firewall configuration and rules.	No exceptions noted.
CC 6.6.2	Remote access to in-scope production systems occurs over a secure encrypted protocol and requires multi-factor authentication.	We inspected the company's VPN configuration settings to verify multi-factor authentication.	No exceptions noted.
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC 6.7.1	The service environment firewall restricts outbound network traffic to only those services specifically required for service operation and all those services include encryption, and authentication.	We inspected the company's firewall configuration settings for outbound network traffic.	No exceptions noted.
CC 6.7.2	The service limits user data transmission to only events initiated via an authenticated and authorized user request.	We inspected the company's authentication system to review data transmission limitations.	No exceptions noted.
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			

CC 6.8.1	All servers perform file integrity monitoring to identify and track the presence of any unauthorized files such as malware or other unauthorized files.	We inspected the company's file integrity monitoring system for any alerts.	No exceptions noted.

CC 7.0 Common Criteria Related to System Operations

Control Ref	Control Activity	Test Performed	Test Results
CC 7.1 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.**			
CC 7.1.1	The company performs quarterly internal and external vulnerability scans and remediates all findings based on risk.	We inspected the company's vulnerability scans to include any findings.	No exceptions noted.
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC 7.2.1	The company has implemented continuous Intrusion Detection Monitoring, and System Availability monitoring via Nagios with critical alerts immediately escalated to technical staff.	We inspected the company's intrusion detection system configuration and validated it is active.	No exceptions noted.
CC 7.3 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.			

CC 7.3.1	Management reviews all security tickets to determine if there is any indication that a protected classification of data exists outside of the tokenization database and takes immediate remedial action if/as required.	We inspected all incidents to determine if there were any stray data incidents discovered during the period.	There was no control activity to test.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC 7.4.1	The company manages and maintains an incident response plan.	We inspected the company's incident response plan (IRP).	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC 7.5.1	The company's incident response plan includes specific activities to recover from a security incident.	We inspected the company's incident response plan (IRP) to include recovery measures for any security incidents.	No exceptions noted.

CC 8.0 Common Criteria Related to Change Management

Control Ref	Control Activity	Test Performed	Test Results
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			

CC 8.1.1	A formal change management process is in place, which includes ongoing and continuous communication to discuss upcoming changes to the system.	We inspected a sample of the company's change management records to review ongoing communication.	No exceptions noted.

CC 9.0 Common Criteria Related to Risk Mitigation

Control Ref	Control Activity	Test Performed	Test Results
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC 9.1.1	Management performs an annual formal risk assessment exercise the results of which are documented and retained.	We inspected the company's annual risk assessment to include the results at the completion of the assessment.	No exceptions noted.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC 9.2.1	Management performs an annual formal risk assessment exercise, the results of which are documented and retained for vendors and business partners.	We inspected the company's annual risk assessment to include the results at the completion of the assessment for vendors and business partners.	No exceptions noted.

A 1.0 Additional Criteria for Availability

Control Ref	Control Activity	Test Performed	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A.1.1.1	The company uses the data log to monitor system utilization and implements alerts within the system to receive advanced warning of any capacity limits.	We inspected the company's data log system, which monitors utilization and sends alerts when capacity limits are reached.	No exceptions noted.
A.1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A.1.2.1	Management maintains two tandem service implementations, which are geographically dispersed such that the failure of anyone environment will have no impact on the service.	We inspected the client's service footprint, which was tested to have a physical location in Allentown, PA, and Seattle, WA.	No exceptions noted.
A.1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			

A.1.3.1	The entity regularly takes down one or more system environments both for maintenance and testing the service's ability to recover using the other hot running implementation.	We inspected the annual disaster recovery testing activity performed by the company.	No exceptions noted.

C 1.0 Additional Criteria for Confidentiality

Control Ref	Control Activity	Test Performed	Test Results
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C.1.1.1	Management clearly documents confidentiality commitments supported by internal controls within the service's Terms of Service.	We inspected the company's terms of service agreement, which was examined for the existence of confidentiality commitments.	No exceptions noted.
C 1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C.1.2.1	The service enforces a retention policy per each user data element stored, which may be indefinite, or time limited from last data access.	We inspected the company's internal handbook to include the retention of records.	No exceptions noted.

P 1.0 Additional Criteria for Privacy

Control Ref	Control Activity	Test Performed	Test Results
P.2.1 COSO Principle: 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 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.			
P 2.1.1	The company maintains and communicates both a privacy and GDPR notice to all customers.	We inspected the company's GDPR notice to customers.	No exceptions noted.
P 2.2 COSO Principle: 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 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.			
P 2.2.1	The company retains only customer PII that is proactively disclosed via either a web payment form or a 'contact us' website form or customer-initiated email and is retained according to the GDPR Policy, and only for the intended purpose of either being billed or being contacted.	We inspected the company's retained PII records for customers and prospective customers.	No exceptions noted.
P 2.3 COSO Principle: Personal information is collected consistent with the entity's objectives related to privacy.			

P 2.3.1	The company retains only customer PII that is proactively disclosed via either a web payment form or a 'contact us' web site form or customer-initiated email and is retained according to the GDPR Policy, and only for the intended purpose of either being billed or being contacted.	We inspected the company's retained PII records for customers and prospective customers.	No exceptions noted.
P 2.4 COSO Principle: 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 consent prior to the collection of the information to meet the entity's objectives related to privacy.			
P 2.4.1	The company website in compliance with GDPR requires the explicit consent of visitors prior to using tracking cookies and allows to the non-consent thereof with an explanation of consequences for non-consenting.	We inspected the consent records that are advertised to customers on the company's website.	No exceptions noted.
P 2.5 COSO Principle: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P 2.5.1	The company retains only customer PII that is proactively disclosed via either a web payment form or a 'contact us' web site form or customer-initiated email and is retained according to the GDPR Policy, and only for the intended purpose of either being billed or being contacted.	We inspected the company's retained PII records for customers and prospective customers.	No exceptions noted.
P 2.6 COSO Principle: The entity retains personal information consistent with the entity's objectives related to privacy.			

P 2.6.1	The company retains only customer PII that is proactively disclosed via either a web payment form or a 'contact us' web site form or customer-initiated email and is retained according to the GDPR Policy, and only for the intended purpose of either being billed or being contacted.	We inspected the company's retained PII records for customers and prospective customers.	No exceptions noted.
P. 2.7 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P 2.7.1	The entity performs deletion in accordance with vendor best practices for database data removal such that the data is not recoverable by the entity or anyone else.	The company had no data removal requests for the period.	There was no control activity to test.
P 2.8 The entity grants identified, and authenticated data subjects the ability to access their stored personal information for 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.			
P 2.8.1	The entity verifies data subjects may request and receive an inventory and accounting of data retained by them by emailing 'compliance@auricsystems.com'.	We inspected all inquiries sent to compliance@auricsystems.com during the period, but there was no activity during this period.	There was no control activity to test.
P 2.9 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 objectives related to privacy.			

P 2.9.1	The entity verifies data subjects may request and receive an inventory and accounting of data retained by them by emailing 'compliance@auricsystems.com'.	We inspected all inquiries sent to compliance@auricsystems.com during the period, but there was no activity during this period.	There was no control activity to test.
P 2.10 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 related to privacy.			
P 2.10.1	The entity does not disclose information to third parties, including without consent.	We inspected the population of all third-party disclosures at the organization and determined there was no control activity for the period.	There was no control activity to test.
P 2.11 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.			
P 2.11.1	The entity does not disclose information to third parties, including without consent.	We inspected the population of all third-party disclosures at the organization and determined there was no control activity for the period.	There was no control activity to test.
P 2.12 The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			
P 2.12.1	The entity creates and retains accurate and timely recording of unauthorized disclosures per its GDPR policy.	We inspected any recording of unauthorized disclosures and determined there was no control activity for the period.	There was no control activity to test.
P 2.13 The entity obtains privacy commitments from vendors and other third parties whose products and services are part of the system and who have access to personal information processed by the system that are consistent with the entity's privacy commitments and system requirements.			

P 2.13.1	The entity's subcontractors or third parties with access to sensitive data have formal agreements ("Data Processing Agreements") clearly defining information security and privacy responsibilities.	We inspected the company's data processing agreements to third parties or subcontractors and determined there was no control activity for the period.	There was no control activity to test.
P 2.14 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 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.			
P 2.14.1	The entity's subcontractors or third parties with access to sensitive data have formal agreements ("Data Processing Agreements") clearly defining information security and privacy responsibilities.	We inspected the company's data processing agreements to third parties or subcontractors and determined there was no control activity for the period.	There was no control activity to test.
P 2.15 The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
P 2.15.1	The entity provides notifications of breaches and/or privacy per its GDPR policy.	We inspected all breaches at the company during the period and determined there was no control activity for the period.	There was no control activity to test.
P 2.16 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.			
P 2.16.1	The company verifies data subjects may request and receive an inventory and	We inspected all inquiries sent to compliance@auricsystems.com during	There was no control

	accounting of data retained by them by emailing 'compliance@auricsystems.com.'	the period and determined there was no control activity for the period.	activity to test.
P 2.17 The entity provides to the data subjects an accounting of the personal information held and disclosure of a data subject's personal information, upon the data subject's request, consistent with the entity's privacy commitments and system requirements.			
P 2.17.1	The company verifies data subjects may request and receive an inventory and accounting of data retained by them by emailing 'compliance@auricsystems.com.'	We inspected all inquiries sent to compliance@auricsystems.com during the period and determined there was no control activity for the period.	There was no control activity to test.
P 2.18 The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
P 2.18.1	The company retains only customer PII that is proactively disclosed via either a web payment form or a 'contact us' web site form or customer-initiated email and is retained according to the GDPR Policy, and only for the intended purpose of either being billed or being contacted.	We inspected a sample of the company's retained PII records for customers and prospective customers.	No exceptions noted.
P 2.19 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 to identified deficiencies are made or taken in a timely manner.			

P 2.19.1	The company verifies data subjects may request and receive an inventory and accounting of data retained by them by emailing 'compliance@auricsystems.com.'	We inspected all inquiries sent to compliance@auricsystems.com during the period and determined there was no control activity for the period.	There was no control activity to test.
P 2.20 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 to identified deficiencies are made or taken in a timely manner.			
P 2.20.1	The company verifies data subjects may request and receive an inventory and accounting of data retained by them by emailing 'compliance@auricsystems.com.'	We inspected all inquiries sent to compliance@auricsystems.com during the period and determined there was no control activity for the period.	There was no control activity to test.