System and Organization Controls 2 (SOC 2) Type 2

Report on controls placed in operation at ESW Operations, LLC relevant to Security and Availability and the suitability of the design and operating effectiveness of its controls

For the Period October 1, 2023 to September 30, 2024

TABLE OF CONTENTS

Section 1

Section 2

Section 3

Section 4

Section 5

SECTION ONE

Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of ESW Operations, LLC
Austin, TX

Scope

We have examined ESW Operations, LLC's ("Service Organization" or "ESW" or "ESW Company") accompanying description of its CloudFix, Jive (an IgniteTech Solution), Aurea DCM (Distribution Channel Management, ADCM), AlertFind (MessageOne, M1, AMS), XANT (InsideSales, Playbooks, PB), Bonzai Intranet, Aurea CRM (ACRM, Update), Engine Yard, and Influitive (PostBeyond) systems ("ESW Product Platforms") found in Section 3 titled "ESW Operations, LLC's Description of its ESW Product Platforms" throughout the period October 1, 2023 to September 30, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA*, Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that ESW's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria.*

The information included in Section 5, "Other Information Provided by ESW Operations, LLC," is presented by ESW's management to provide additional information and is not a part of ESW's description of its ESW Product Platforms made available to user entities during the period October 1, 2023 to September 30, 2024. Information about ESW's management responses to testing exceptions has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

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

Service Organization's Responsibilities

ESW 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 ESW's service commitments and system requirements were achieved. In Section 2, ESW has provided the accompanying assertion titled, "Assertion of ESW Operations, LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ESW is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. 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 a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- 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.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual 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 or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, “Trust Services Criteria, Related Controls and Tests of Controls” of this report.

Opinion

In our opinion, in all material respects:

a) The description presents ESW’s ESW Product Platforms that was designed and implemented throughout the period October 1, 2023 to September 30, 2024 in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that ESW’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 ESW’s controls throughout that period.

c) The controls stated in the description operated effectively throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that ESW’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complimentary user entity controls assumed in the design of ESW’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 ESW, user entities of ESW’s ESW Product Platforms during some or all of the period October 1, 2023 to September 30, 2024, business partners of ESW subject to risks arising from interactions with the ESW Product Platforms, 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 the specified parties.

CyberGuard Compliance, LLP

Las Vegas, NV
November 22, 2024

SECTION TWO

Assertion of ESW Operations, LLC Management

ASSERTION OF ESW OPERATIONS, LLC MANAGEMENT

November 22, 2024

Scope

We have prepared the accompanying description of ESW Operations, LLC's ("Service Organization" or "ESW" or "ESW Company") CloudFix, Jive (an IgniteTech Solution), Aurea DCM (Distribution Channel Management, ADCM), AlertFind (MessageOne, M1, AMS), XANT (InsideSales, Playbooks, PB), Bonzai Intranet, Aurea CRM (ACRM, Update), Engine Yard, and Influitive (PostBeyond) systems ("ESW Product Platforms") titled "ESW Operations, LLC's Description of its ESW Product Platforms" throughout the period October 1, 2023 to September 30, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) in AICPA, Description Criteria*, (description criteria). The description is intended to provide report users with information about the ESW Product Platforms that may be useful when assessing the risks arising from interactions with ESW's system, particularly information about system controls that ESW 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 and Availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria*.

ESW uses a subservice organization to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ESW, to achieve ESW's service commitments and system requirements based on the applicable trust services criteria. The description presents ESW's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ESW's controls. The description does not disclose the actual controls at the subservice organization.

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

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

1) The description presents ESW’s ESW Product Platforms that was designed and implemented throughout the period October 1, 2023 to September 30, 2024 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that ESW’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 ESW’s controls throughout that period.
3) The controls stated in the description operated effectively throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that ESW’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complimentary user entity controls assumed in the design of ESW’s controls operated effectively throughout that period.

ESW Operations, LLC

SECTION THREE

ESW Operations, LLC’s Description of its ESW Product Platforms

ESW OPERATIONS, LLC'S DESCRIPTION OF ITS ESW PRODUCT PLATFORMS

1 Overview of ESW Operations, LLC's Operations

Company Background

ESW Operations, LLC

ESW Operations, LLC (ESW) is a software company that enables companies to deliver transformative customer experiences. The ESW Product Platforms (ESW) help customers build, execute, monitor, and optimize the end-to-end customer journey in a diverse range of industries including energy, retail, insurance, travel and hospitality, as well as in industry-agnostic business environments.

Description of Services Provided

Aurea DCM (Distribution Channel Management, ADCM)

For the front office, DCM is designed to deliver services that provide producers a seamless and empowering experience, from getting started to getting paid. DCM is designed to simplify producer commission modeling, calculation, and processing for insurers, and provides multiple producer manager functions. Insurance carriers create maximum visibility around compensation management to avoid confusing commission payouts and the costly sales downtime they create.

The automated job scheduling system is configured to log successful and failed job activity. Job scheduler configuration showing that job scheduler is configured to log successful and failed job activity. Escalation procedures are in place to guide operations personnel in the event of a job failure. Errors identified from Job Monitoring are sent to the SaaS Ops team for tracking.

1) *Centralized commission calculation and payment*
   Streamline and centralize compensation calculation and management. With DCM, producers and agencies are assured payment accuracy and timeliness, giving producers confidence to focus on their business.

2) *Compliance visibility and confidence*
   Achieve complete visibility, 100% automated compliance, and out-of-the-box integration with all federal and state regulatory agencies, including NIPR and FINRA.

3) *Increase back-office productivity*
   To keep pace with today's industry, insurers need to easily automate the processes and workflows that drive their business. DCM streamlines key insurance workflows, like producer onboarding, dispute resolution, and more.

4) *Tap into the power of Enterprise*
   The Enterprise edition of DCM combines easier-to-use producer commission modeling with powerful calculation and processing and delivers end-to-end workflow automation for key insurance processes.

AlertFind (MessageOne, M1, AMS)
The AMS AlertFind Services system is a hosted cloud-based Software as a Service (SaaS) Solution that delivers communications during emergencies and unplanned disruptions. Notifications can be sent safely and securely to employees via fax, email, landline, mobile phone, Short Message Service (SMS) text message, or mobile applications and allows them to respond. This allows companies to verify the safety of their employees in emergency situations. Being hosted, clients do not need to install anything on their infrastructure, and this provides the necessary resiliency in case of disaster to the company's own systems.

XANT (InsideSales, Playbooks)
Playbooks is a sales acceleration platform for sales representatives to use on their web browser. Playbooks continuously gathers actionable insights about companies in the sales representatives' patch and makes the most relevant information available when needed. In addition, Playbooks automatically synchronizes sales activities, prospecting, and pipeline-building sales tools, as well as recording sale interaction data to the customer relationship management (CRM) without manual data entry. Playbooks prioritizes and manages leads and accounts with personalized sales engagement plans by using Neuralytics, the predictive analytics engine built on over 100 billion sales interactions, to analyze and determine when leads are most likely to engage, and it integrates contact prospects with telephony and e-mail.

Jive
The Jive innovative platform is an IgniteTech Solution proven to be a leader in accelerating workplace digital transformation for organizations, enabling people to work better together, driving productivity, improving collaboration and modernizing search. The industry-leading Interactive Intranet and Customer Community solutions connect people, information, and ideas to help businesses outpace their competitors. With more than 30 million users worldwide and customers in virtually every industry, Jive is consistently recognized as a leader by top analyst firms.

Bonzai Intranet
Bonzai Intranet technology platform is built on Microsoft SharePoint and SAP (Systems, Applications, and Products) to enable companies to engage and manage employees across a diverse range of industries including energy, retail, insurance, health, travel, and finance. Bonzai Intranet provides an end-to-end project management suite of tools that include project scheduling, timesheets, resource management, and cost management. In addition, Bonzai Intranet offers a self-service Human Resources (HR) solution built-on SAP as well as intranet solutions that include social feeds, news, video, ideas, employee recognition, and knowledge management.

Aurea CRM (ACRM)

Aurea CRM is a CRM solution to manage every interaction with its customers throughout their journey. Offering both web-based and mobile capabilities, Aurea CRM lets its clients create a 360-degree view of every customer.

Engine Yard

Engine Yard Cloud (EYC) is a Platform-as-a-Service (PaaS) for deploying and managing applications and infrastructure resources in the cloud. EYC runs applications on a fully managed Cloud infrastructure. It is designed to allow developers to shift from DevOps to NoOps, as they don't need to spend additional time on deployments aside from a single click on the UI. The platform provides a secure, full-stack environment for customers' applications which includes monitoring, load-balancing, and auto-scaling. EYC provides a full-blown web console and CLI that customers use to define and configure their applications as well as other cloud resources. They can provision and leverage additional cloud resources in their application including databases, storage, and caching. The platform gives any developer access to easily deploy scalable, reliable applications on a robust platform that also includes 24x7 customer support

CloudFix

CloudFix is an Automated AWS Cost Optimization application that finds opportunities for reducing costs in its client's AWS account and then makes the necessary changes on the client's behalf once the client has given approval.

Influitive/PostBeyond

PostBeyond is an innovative employee advocacy platform designed to transform employees into powerful social advocates for their organizations. By providing a centralized content library with simple approval workflows, personalized content feeds, and AI-powered content generation, the platform enables businesses to seamlessly amplify their brand visibility across social media channels. Employees can easily share pre-approved content, schedule posts, and engage with their networks, while administrators gain access to robust analytics and reporting tools that track program performance. The platform goes beyond mere content sharing by incorporating strategic engagement mechanics, such as rewards for shares and interactions, ultimately helping companies leverage their workforce's social networks to drive brand awareness, business opportunities, and authentic storytelling.

Principal Service Commitments and System Requirements

Company's security and availability commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service document published on the customer-facing website. The principal security and availability commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the in-scope applications and the customer data in accordance with ESW's security requirements
- Perform annual third-party security and compliance audits of the environment.
  - Reporting on Controls at a Service Organization Relevant to Security or Availability (SOC 2) examinations
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of ESW personnel with access to any production systems
- Prevent malware from being introduced to production systems
- Continuously monitor the production environment for vulnerabilities and malicious traffic
- Use industry-standard secure encryption methods to protect customer data at rest and in transit
- Transmit unique login credentials and customer data via encrypted connections
- Maintain an availability SLA for customers of 99.5% uptime for each calendar quarter
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes
- Maintain and adhere to a formal incident management process, including security incident escalation procedures

ESW Company establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in ESW's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

The Company regularly reviews the Security, Availability, and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of the mentioned commitments within the agreement, ESW will notify the customer via the ESW or other company's websites, Customer Support channels or directly via email.

2 Overview of the System and Applications

Scope and System Boundaries

As outlined in *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* a system is designed, implemented, and operated to provide reasonable assurance that ESW's service commitments and system requirements are achieved.

The scope of this examination is limited to ESW's: CloudFix, Jive (an IgniteTech Solution), Distribution Channel Management, MessageOne (AlertFind, M1, AMS), XANT (InsideSales, Playbooks, PB), Bonzai Intranet, ESW CRM (ACRM, Update), Retail Energy Billing (AES), Engine Yard Systems ("ESW Product Platforms"). The specific criteria and related control activities included in the scope of this engagement can be found in Section 4.

All criteria and controls within the availability category are applicable to the ESW Product Platforms. See page 38 for Non-Applicable Trust Services Criteria relating to security.

System Overview

The System is comprised of the following components:

- ***Infrastructure*** **-** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** **-** The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** **-** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** **-** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures*** **-** The automated and manual procedures involved in the operation of a system

Infrastructure

ESW has remote employees worldwide, for engineering and operations support. The Company headquarters are located in Austin, Texas.

ESW systems utilizes Amazon Web Services (AWS), for their data center hosting services in the following regions:

- AWS Data Center (North American Geographic Zone) - North Virginia
- AWS Data Center (EU Geographic Zone) Ireland

ESW systems are hosted in Amazon Web Services (AWS) across multiple Availability Zones for redundancy and disaster recovery purposes. ESW does not own or maintain any hardware in the AWS Data Centers. Services operate within a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure, and ESW is responsible for securing the ESW Product Platforms deployed in AWS (e.g., IAM, S3 bucket policies, Operating System and application security, Security Group configuration, network traffic monitoring).

ESW uses a different AWS account to separate the containerized production, staging, and development environments. Access to AWS production instances is allowed only through an encrypted MFA VPN from the ESW's corporate network to ensure the privacy and integrity of data transmitted over the public network. VPN connections are whitelisted to ESW's IPs and are secured using AES-256 bit or greater encryption. Access is restricted to authorized administrators, who must authenticate via a bastion host through a secure SSH key, AWS IAM roles, and multi-factor authentication.

Production instances at AWS are logically separate from ESW's internal corporate network. All container hosts and database servers run on EC2 instances within Auto Scaling groups. AWS CloudFormation provides auto-scaling management of the production systems based on a defined template, which allows Integrate to deploy and configure consistently hardened instances.

All container hosts and database servers run on EC2 instances that are secured via Security Groups. Security Groups monitor incoming network traffic by analyzing data packets and filtering traffic based on an Integrate-defined ruleset. Access to manage the Security Groups is restricted to authorized DevOps personnel, and changes to these rulesets are governed by the ESW's change management policy, which includes documenting, testing, and approving the change.

Software

The users interact with the systems using different web app or API components.

ESW uses a few AWS systems and services (Amazon Cognito, AD/DAP) to authenticate users and to secure communication between components. All the database access (Amazon DynamoDB) is made through AWS AppSync requests from the web app and the different backends containers. All GraphQL API interactions persist in Amazon S3 for analytics purposes.

ESW uses multiple software and utilities to configure, develop, and support the in-scope infrastructure and applications, including:

- *AWS Lambda* – Serverless compute service
- *Docker* – Container engine
- *Docker Hub* – Container image repository

- *GitHub* – Online source code control repository
- *Jenkins* – Continuous integration platform

Data

a) Aurea DCM

Producer Data

DCM is the system of record for agents and agencies. These producers are onboarded in DCM and set up in a hierarchy. DCM also houses their State Licenses and Appointments, which are downloaded from the third-party system, NIPR. Similarly, the continuing education information for these agents is provided to DCM by a third-party system. The data is stored in DCM for compensation reasons and is not modified in DCM.

Insurance Policies

This data contains basic policy information (e.g., client name, issue date, product, etc.), agent and agency sold/servicing that policy, group counts, member counts, and compensation rule for those agents/agencies. This data is managed in clients' systems -- i.e., DCM is not the system of records for this data. As a result, DCM does not modify this data.

Insurance Premiums

DCM receives premium transactions from clients; this triggers commission calculations in DCM for the respective policies and associated agents/agencies.

Compensation

The commission data is sent back to clients' systems during nightly batch cycles. Furthermore, client users can issue manual payments to agencies in DCM. These manual payments are also sent to clients' systems during the nightly batch cycle.

Data Communications

A network diagram is documented that defines an objective description of the system. The internal network is protected from public internet traffic via AWS security settings that contain an implicit '*deny all*' function, and only specific services are allowed to specific destinations. AWS ELB implicitly masks the IP addresses of internal servers in VPC. Access to administer the ESW AWS environment is restricted to personnel commensurate with their job responsibilities.

The Hypertext Transfer Protocol Secure (HTTPS) and Secure Sockets Layer (SSL) encryption protocol is utilized to encrypt data communications via remote internet sessions to the internal network to ensure the privacy and integrity of the data being passed over the public network.

The internal network is designed to be segmented from the production environment. With this segmentation, data communication architecture has been constructed in which production services are intentionally separated from any unauthorized internal or external access.

b) AlertFind

The AMS AlertFind Services system runs in Docker containers in Amazon Elastic Compute Cloud (EC2) instances that provide scalable computing capacity in the AWS cloud. These servers are running in four Virtual Private Clouds (VPCs), two in the United States and two in Europe, within the AWS environment.

The Docker containers are currently running within three Docker Hosts of type AWS x1.32 in the United States (US) and one Docker Host of type AWS x1.32 in the European Union (EU).

Secure Shell (SSH) access to Docker Host is restricted to operators of the central infrastructure SaaS Operations (SaaS Ops) team. For the Amazon EC2 instances, access is based on controlled SSH keys. Data is stored in Amazon Elastic Block Store (EBS) volumes providing persistent block storage volumes. EBS volumes are automatically replicated within their respective AWS availability zones to protect against component failure, resulting in high availability and durability.

Access to the Aurora Postgres database is restricted to personnel commensurate with their job responsibilities.

<u>Client Setup Data</u>

Periodically, for some clients, the roster file import procedure is executed:

- The client sends a text file with the names and contact information (like emails and phone numbers) to a secured FTP server.
- Client Support executes a semi-automatic procedure to import the information into the system, including the execution of import tools.
- Temporary files are removed from the server.
- For clients that use both AMS AlertFind and AMS Email Continuity and Email Archival, the systems are integrated to share users. Alternatively, other clients use a tool called AF-Connector, which connects to the client’s system providing contact information. Access to client data is restricted to client support agents only.

<u>Alerts Notification Data</u>

When a notification is required to be sent the AlertFind notification agent in charge of sending such notifications can log into AlertFind and trigger the notification. Notifications can be sent to all users, or a subset of users based on group assignment or location.

The elements that typically make up a notification are:

- Recipients
- Subject
- Language
- Attachments
- Message
- Response

Once the notification is ready it will be sent based on the recipient’s preferences using one of the following channels:

- SMS Text Message
- Voice Message - Text to speech is used here to narrate the message.
- Email
- Fax
- Pager
- AlertFind Mobile Application (available on Android or Apple’s iOS)
- On the receiving end, the user can reply to the notification to confirm receipt as well as indicate their safety status.

c) XANT

The data captured in the Playbooks system includes customer business data, including names, addresses, telephone numbers, and e-mail addresses. Customer data is considered restricted (or confidential) data. As such, this is governed by the confidentiality agreements executed between XANT and customers or vendors. XANT’s information classification and handling requirements are defined in the data management and classification policy. This policy has four categories, including: public, non-public, protected, and restricted. Restricted data requires the highest level of security in accordance with relevant security policies, regulations, and contractual requirements.

Data within the Playbooks system is generated and uploaded by Playbooks customers. The transmission of confidential data is secured via an internet connection encrypted with TLS protocol. Each customer is responsible for administering their users and data which includes the accuracy and timeliness of the data entered into the system.

Customers can retrieve reports related to their respective environments via the Playbooks system. Customers can report operational failures, incidents, system problems, concerns, and user complaints by communicating with the systems team by opening a ticket in the Lead Management Platform (LMP) or on the XANT website. Policies are published on the Company intranet and contact information is available to clients on the Company public website.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Information on corporate security that may include the following: • Asset protection • Technology acceptable use • Data management and classification • Data storage and transmission • Access control	XANT standard operating process and procedures	Non-Public
Customer data may include the following (depending upon the scope of services provided): • Name • Address • Telephone number • E-mail addresses	Provides the following data (depending upon the scope of services provided) in various exports and reports: • Customer profiles • Dashboards and customer interaction history	Restricted

d) Jive

Application source code data is a critical component to provide application services to Jive's customers. The application source code is stored within the source code management system which only authorized development personnel have the ability to access and modify. The ability to migrate changes into the production environment is restricted to authorized personnel and is managed by configuration management software. Jive has implemented a demo environment and client production data is not utilized in development or testing.

Customers are responsible for inputting and managing their data on their instance of the Jive application via an Internet connection. Jive uses encryption to protect transmitting data over non-trusted networks. Customers implement transport layer security (TLS) or VPN technology to encrypt the network traffic to and from their hosted application. All AWS customers will have encryption-at-rest by default.

Jive has defined confidential data relevant to the AWS based Jive-n System and cloud services system as customer data and confidential information maintained within the system. As such, this is governed by the confidentiality agreements executed between Jive and customers or vendors.

Jive's information classification and handling requirements are defined in the data classification and handling policy. The policy has four categories which include the following: Jive Public, Jive Non-Public, Jive Confidential, and Customer Data. Customer data requires the highest level of security and is held in accordance with the relevant security policies, regulations, and contractual requirements. All customer data is treated as confidential and is subject to Jive's End User License Agreement (EULA).

Jive commits to protecting customers' confidential information. In addition to the product overview documents, confidentiality commitments, including non-disclosure agreements (NDAs), are documented in the customer contract agreement that customers sign prior to sharing any confidential data. Confidentiality agreements with third parties are documented and enforced prior to sharing any confidential data. Confidential information is stored and made available to customers based upon the predefined retention periods and in accordance with the retention commitments.

Documented data disposal policies are in place to help guide personnel in the disposal of confidential information. SaaS Ops personnel dispose of customer data from production databases upon termination of the services in accordance with the disposal commitments. In AWS, the virtual customer instances are deleted upon contract termination, rendering the data inaccessible and unrecoverable within 90 days, once the data has aged out of the backups.

e) Bonzai Intranet

Customer Data
Bonzai does not store customer data in its own systems; rather, customer data is stored in the customer's own SharePoint and database areas.

Bonzai Settings
Bonzai stores theme information in its Brick system hosted in AWS S3. Information is encrypted at rest and during transmission and requires authentication via Amazon Cognito.

f) ACRM

CRM product suite included the following components:

1. *ACRM.Web* (Asp.net web application, which can be hosted on the internet information server. This need windows server machine to run)
2. *ACRM.Designer* (Asp.net web application, which can be hosted on the internet information server. This need windows server machine to host)
3. *ACRM.Win* (This is set of tools, which can run on windows machines)
4. *ACRM.Connectors* (These are set of windows services, used to synchronize emails to CRM)

5. *ACRM.Interface* (Asp.net web application, which can be hosted on the internet information server. This need windows server machine to run)
6. *ACRM.WebServices* (Asp.net web application which can be hosted on the internet information server. This needs windows server machine to run)
7. *ACRM.ConnectLive* (Outlook plugin for CRM)
8. *ACRM.Launcher* (Windows-based app & service, need to install in all the client machines using the ACRM.Web)
9. *ACRM.WebOffline* (Same as ACRM.Web, but this runs on local client machine under IIS Express)
10. *ACRM.OfficeAddin* (MS Word Addin for CRM)

The product uses MSSQL and Oracle database for storing the data. The usage of Oracle database is optional. There are two databases used in CRM: designer db and CRM db. designer db can be only MSSQL and CRM db can be MSSQL or Oracle.

The app can be either installed via installers shipped as part of the product suite or via copying the files from zip packages.

g) Engine Yard

Engine Yard Kontainers (EYK) is a Platform-as-a-Service (PaaS) for deploying and managing applications in containers. EYK runs application containers on a fully managed Kubernetes infrastructure. It is designed to allow developers to shift from DevOps to NoOps, as they don’t need to spend additional time on deployments aside from a single code push command. EYK leverages existing configuration management command-line interface (CLI) to run deployments using a new remote EYK target. The platform provides a secure, full-stack environment for customers’ applications which includes monitoring, load-balancing, and auto-scaling. EYK provides a simple web console and CLI that customers use to define and configure their applications. They can provision and leverage additional cloud resources in their application including databases, storage, and caching. The platform gives any developer access to easily deploy scalable, reliable applications on a robust platform that also includes 24x7 customer support.

h) CloudFix

CloudFix connects to the customer AWS account and collects data about resources, cost, usage and metrics. The data is examined and cost savings opportunities are created for the user to approve. Approved opportunities trigger workflows that make updates to the AWS account.

CloudFix is divided into two divisions:

- Customer dashboard
  Internal leaderboard showing tenants with most recommended savings for the used AWS services.

- Available actions:
  Implement or cancel recommended savings.

  The basic data flow of CloudFix currently is as follows:

  - *Setup*
    With one click, customers install a CloudFormation template in their accounts which creates roles for CloudFix, configures AWS Config (if necessary) to dump snapshots into a bucket and updates to an SNS topic

  - *Data Collection*
    The CloudFix backend then reads the snapshots to create a Neptune graph of the customer's resources (one graph per customer, including all the customer's AWS accounts). It also calls CloudWatch APIs to populate an S3 bucket. In addition, CloudFix also consume updates from AWS Config to update Neptune.

  - *Opportunity Finding*
    Periodically, another flow is run to pull resource data and CloudWatch APIs to update these two. After resource collection, a finder processes the collected data and generates opportunities. These are then enriched with cost savings estimates, etc. The enriched opportunities are used to generate or update recommendations which are shown on a UI

  - *Opportunity Fixing*
    Once users approve fixes, APIs are called to execute them using another flow.

i) Influitive/PostBeyond

Platform Overview
PostBeyond is a cloud-native employee advocacy platform hosted on AWS, designed to enable seamless social media content sharing and engagement for enterprises.

Technical Infrastructure

- *Compute Services*
  - Backend Framework: Python Flask
  - Hosting Platform: Amazon Linux
  - Deployment: AWS EC2 instances across multiple availability zones
  - Scalability: Elastic infrastructure supporting auto-scaling

- *Storage* Architecture
    - Static Content: Amazon S3
    - Content Distribution: AWS CloudFront
    - Backup: Redundant storage with versioning
- *Database*
    - Primary Database: MySQL RDS
    - Database Hosting: AWS Managed Relational Database Service

- *Core* Platform Modules
    - Daily Post Management
    - Content Suggestion Engine
    - Administrative Dashboard
    - Social Media Sharing Mechanism
    - Advanced Analytics
    - Business Intelligence Event Capture
    - Authentication System
    - Email Notification Service
    - Post Queuing Functionality
    - Bulk Post Creation
    - User Inbox

- *Mobile* Compatibility
    - iOS: Version 13+
    - Android: SDK Version 21+

- *Security* Considerations
    - Role-Based Access Control
    - Encrypted data transmission
    - Compliance with enterprise security standards

People

ESW's HR provider is Crossover.com. They are hiring people all over the world except embargo countries. Also, they conduct all needed background checks. The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

- *Executive Management* oversees, and is ultimately responsible for, all aspects of service delivery and security commitments. Among other responsibilities, Executive Management ensures that controls are enforced, risk assessment/management activities are approved and prioritized, people are appropriately trained, and systems and processes are in place to meet security and service requirements.

- *Human Resources (Crossover)* is responsible for managing all functions related to recruiting and hiring, employee relations, performance management, training, and resource management. Human Resources partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with ESW Company's mission, vision, and values.

- *Information Technology (IT)* management has overall responsibility and accountability for the enterprise computing environment. DevOps personnel administer systems and perform services supporting key business processes, including architecting and maintaining secure and adequate infrastructure, monitoring network traffic, and deploying approved changes to production. The Engineering team is responsible for application development, initial testing of changes, and troubleshooting/resolving application issues.

- *Information Security and Compliance* is responsible for performing assessing and managing risk, defining controls, monitoring performance of security controls, addressing and responding to security incidents, maintaining and communicating updates to security policies, and conducting security awareness training of all users.

- *Customer Success Managers (CSM)* are responsible for initiating the creation of new customer setups on the ESW Product Platforms, adding users to new customer setups, providing user documentation to and coordinating training for new customers, and overall management of the account to ensure continued customer satisfaction.

- *Customer Support* is responsible for creating new customer setups on the ESW Company System platform, fielding customer calls regarding the ESW Company System services, initiating and responding to help desk tickets based on customer requests, and communicating with customers regarding any issues or outages.

ESW Company is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. ESW Company endorses a work environment free from discrimination, harassment, and sexual harassment.

<u>Procedures</u>

ESW has a Chief Information Security Officer (CISO) who is responsible for the design and oversight of security and privacy initiatives. The CISO reports directly to the COO and indirectly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, and operation of the ESW Product Platforms. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CISO.

All employees are expected to adhere to the Company IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect ESW's service commitments or system requirements.

3 Trust Services Criteria and Related Controls

ESW's criteria and related control activities are included in Section 4 of this report to eliminate the redundancy. The description of the service auditor's tests and the results of those tests are also presented in Section 4, adjacent to the service organization's control activities. The description of the tests and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Control Environment

Management's Philosophy and Operating Style

ESW Company'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.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ESW Company's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of ESW Company's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice.

Employees are provided with an Employee Handbook upon hire, which explains corporate values and code of conduct. Employees acknowledge that they have read, understand, and agree to abide by these values and behavioral standards for the duration of their employment with ESW Company.

SAFE Committee Oversight

ESW's Security Committee is called the Security Assessment & Fulfillment Ensemble (SAFE) Team. SAFE membership is made up of business representatives and is responsible for providing support for the business by ensuring the confidentiality, integrity, and availability of the information and systems with respect to ESW's clients and employees.

Commitment to Competence

Management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. ESW Company has focused on hiring experienced employees for the various positions required for the business.

Organizational Structure and Assignment of Authority and Responsibility

ESW Company's organizational structure provides the framework within which its activities for achieving entity- wide objectives are planned, executed, controlled, and monitored. ESW Company's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. ESW Company has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Customer Access Management

ESW Company provides customers with access to the ESW Product Platforms to access data and statistics. As part of the new customer onboarding process, the assigned Customer Success Manager (CSM):

- Provides documented procedures pertaining to use of the portal
- Facilitates customized training for new customers on the ESW System platforms
- Provisions user accounts based on channels/products in contract. This process triggers emails to the users, in which they are prompted to create their own password based on system-enforced parameters.
- Assigns administrator-level permission to one authorized user account. Once an administrator-level user account has been created for the customer, that administrator can perform user administration activities, including provisioning and revoking access to the ESW System portals.
- *Customer/User:* user which owns the subscription or members of his organization acting as:
  - Administrator role
  - Moderator role
  - Member role

Internal Access Management

Access to IT resources is granted based on role and business justification. Predefined groups are used to assign role-based access privileges and segregate duties and access to systems and data. The Product Security team is responsible for the approval and assignment of access on a need-to-know basis. The granting and removal of access is facilitated through the ITOps team. The ITOps team is responsible for administering and enforcing access to IT resources, as well as user provisioning and deprovisioning. Third-party partners and contractors are authorized prior to the issuance of credentials to access the IT environment.

User accounts for employees, third-party partners, and contractors that are no longer needed are communicated to the Engineering Product team and are immediately disabled. In addition, a review of all user accounts and privileges is performed semi-annually. Inappropriate access is immediately modified or removed.

Administrative privileges to IT resources are granted based on role and business justification and require specific authorization by the management level. Employees requiring administrative access are assigned privileges through group membership or to their unique user account. Access to any database containing confidential data, including access by applications, administrators, and all other users, is restricted through programmatic methods (application code, system utilities). Application service IDs can only be used by applications and not individual users or processes.

All employees and third parties are assigned a unique user ID and authentication credentials aligned with password configuration requirements defined in the Information Security Policy. Password configuration requirements enforce minimum length, password complexity, password expiration, and password history. Group, shared, and generic accounts are prohibited unless specifically required and approved by the Security team. Shared user IDs for system administration activities and other critical functions are not used.

Multi-factor authentication (MFA) is enforced to access production instances through administrative non-console access, remote access, and access to the AWS cloud. MFA requires the use of valid login and time-based token.

Production Access Management

Access to production systems is authenticated using SSH keys and AWS IAM roles, requires multi-factor authentication, and is restricted to authorized administrators. In the event an employee with access to the production environment is terminated, the corresponding AWS IAM roles and SSH keys are removed as a component of the termination process.

Remote Access

Remote access to the network must be authorized and approved and is strictly controlled using public/private keys to access ESW systems. A VPN connection and/or firewall rule is required to access internal services. For employees, automatic disconnect must be configured for remote access technologies after a specified period of inactivity. Remote access for third-party partners and contractors is granted upon authorization for the period needed and is immediately deactivated after use. ESW workstations that remotely connect to ESW’s corporate network must have a strong password, an encrypted hard drive, and an antivirus solution.

Physical Security

The ESW Product Platforms and supporting infrastructure are hosted by AWS.

All physical control and environmental controls for the data center are designed, supported, and tested by AWS.

AWS communicates its security and control environment relevant to customers by doing the following:

- Obtaining industry certifications and independent third-party attestations
- Publishing information about the AWS security and control practices in whitepapers and web site content
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

Physical access to office locations is restricted by badge access. Badges are approved and removed as part of the new hire/termination process. All visitors must sign in and be escorted to office locations.

Third-Party Management

ESW engages with third-party partners to support/extend product offerings. The engagement, management, and monitoring of third-party partners is addressed in the Vendor Management Policy. Prior to engaging with a third-party for the solicitation of services, a signed NDA is received, and due diligence is performed. Annually, vendor risk is assessed as part of the overall risk management effort to ensure continued compliance with the requirements for safeguarding ESW's systems and data.

Third-Party Access

External integrated apps (Google suite, Amazon, Zoom, Zendesk), are invoked by users using the web app. The system receives external integrated apps events in Amazon API Gateway Rest container endpoints and from there persist in the database and in an Amazon S3 bucket for analytics purposes.

Systems Development

ESW follows Software Development and Coding Standards that address security throughout the software development life cycle. Products are developed in accordance with the Agile Software Development Framework. Software development activities are subject to ESW's Change Management Policy and tracked using GitHub.

Developers follow secure coding practices, and all code is reviewed prior to implementation. Coding standards ensure that code is developed securely throughout the development life cycle and security vulnerabilities are addressed. Developers are trained on secure coding techniques.

Development and production environments are segregated. Virtual sandbox and production environments exist in separate virtual networks. The sandbox environment has virtual servers that are separated from production. Sandbox hosts all the lower-level environments (i.e., development, staging). The development environment is used to test code and conduct quality assurance testing. The staging environment is used for customer user acceptance and overall product evaluation. The production environment is used for live applications and data. Role-based access to all three environments is controlled using SSH keys. Access to the production environment is limited to the network administration team. Access to the production environment can be obtained temporarily for troubleshooting by following the defined production access escalation process.

Change Management

ESW Company has documented SDLC and change management procedures, which govern changes to infrastructure, as well as application and API development. Changes to infrastructure and microservices follow a Continuous Integration / Continuous Delivery (CI/CD) model.

The Change Control Policy includes requirements for authorization, testing, approval, and implementation. All changes are requested, tracked, and closed using the internal Jira tickets for product changes and the same system for infrastructure and customer support changes.

All planned and unplanned (emergency) changes must be submitted and approved by the Product Chief Architect. Subsequent to approval, changes are scheduled and communicated to affected parties, including the date/time of the change, anticipated impact to users, and length of downtime, if any.

Change requests are assigned to appropriate IT operations team members for execution. Testing must be completed to confirm the requested functionality has been successfully developed. Assigned individuals are responsible for testing the change in a QA environment. Changes may be implemented into the production environment only after testing has been completed by both the developer and QA Engineer.

Final change approval is obtained by the Product management prior to implementation. Segregation of duties is properly enforced to prevent developers from migrating changes to the production environment. Changes are approved, functionally tested, and include back-out procedures. Upon completion of a significant change, documentation on all relevant requirements implemented on new and/or changed systems is updated as needed.

Patch Management

IT personnel monitor critical vendor patches and upgrades on an ongoing basis to mitigate potential damage to ESW Company's operations resulting from the exploitation of published vulnerabilities. If a patch is deemed necessary, IT personnel document and track the patch installation in a ticket. Critical patches are evaluated and applied within 30 days of release.

Configuration Management

Configuration management tools are used for hardening devices, servers, and databases residing in the cloud infrastructure. These tools enable the automatic configuration of infrastructure devices in accordance with configuration standards. Changes to configurations are logged using GitHub and Jira services. Updates to the configuration management tool are made as needed as new vulnerabilities are identified.

System Monitoring

ESW Company monitors security and operations using network, infrastructure, and database monitoring tools within the ESW System production environment. Agents are installed on all hosts to monitor network security and uptime, disk space, and system resource usage, and alerts are sent to IT personnel for any security events or usage issues. Additionally, audit logs are recorded by the system with a time stamp, are monitored on a regular basis, and are retained according to policy.

Critical events related to the security and availability of the system are logged and monitored at the infrastructure, application, and data layers. ESW also uses anomalous behavior detection/exfiltration software at the infrastructure level to identify personal data exfiltration. Logs provide key information, are indicators of potential compromise, and are used for troubleshooting purposes.

AWS CloudWatch, along with third-party tools, are used to monitor the performance and availability of the infrastructure. CloudTrail and internal Graylog clusters are used to collect and analyze the logs of servers and applications. Logs are reviewed periodically based upon the risk associated with the event and retained in accordance with the Data Retention Policy.

Data Asset Classification and Management

An inventory of all hardware and software located at AWS is maintained and updated as needed. The inventory includes a description of the function/use, version number, and location of all infrastructure hardware. Assets are discovered through an automated scanning process using Qualys, OpenVAS, and Burp for scanning product services. Scans are run on a periodic basis to detect any unauthorized hardware or software.

Data is classified based on value, sensitivity, and use. All ESW information and all information entrusted to ESW from third parties falls into one of four classifications, presented in order of increasing sensitivity.

Information is retained based upon its sensitivity, value, and legal and regulatory retention requirements. ESW considers retention requirements based on the classification and risk assigned. The retention of information applies to both electronic and physical information.

Data Security

TLS, PKI, and AES encryption are used to protect data used, transmitted, and stored. Trusted keys and/or certificates are used for security incident reporting, TLS connections, and interconnections between applications and databases.

Electronic hardware previously used to process or store data must be physically destroyed or wiped using a method that overwrites the data.

A Clean Desk Policy in place to ensure that sensitive/confidential information is secured when not in use. All sensitive/confidential information must be removed from an employee’s user workspace and locked away when the items are not in use or an employee leaves his/her workstation.

Vulnerability Management

Internal and external vulnerability assessments of the ESW Product Platforms are performed on a semi-annual basis and penetration tests of the key systems are performed at least annually. to identify potential security vulnerabilities. If a potential or actual security breach is detected, security personnel work to identify the cause and remediate it immediately. Security personnel reviews the reports and document remediation plans to resolve any potential vulnerabilities, as applicable. Management reviews the results of the report and evaluates updates to the Risk Assessment based on findings.

ESW addresses vulnerabilities potentially affecting the security and availability of systems and data through the following:

- Antivirus software is implemented on all systems commonly affected by malicious software.
- Vendor-supplied security patches are applied as needed. Critical security patches are installed within one month of release.
- Internal and external vulnerability scans run on a semi-annual basis and penetration tests of the key systems are performed at least annually or more frequently as needed due to significant changes in the network.

Issues identified in vulnerability scans and penetration test results are remediated and repeat scans and testing are performed to ensure that weaknesses have been corrected.

Incident Management

ESW has incident response and escalation procedures in place to efficiently and effectively manage unexpected incidents that can potentially impact the business. The incident response process defines activities to identify and mitigate security breaches and manage communications with ESW personnel, as well as customers, legal counsel, or law enforcement as necessary. Actions taken to contain and resolve incidents are documented in a ticketing system. When a security event is detected or reported, IT examines and attempts to resolve the issue and escalates the incident if necessary. Customers are responsible for reporting any security issues based on the terms of the service agreement with ESW.

The Incident Response Policy includes procedures for incident preparation, detection and analysis, notification, containment, eradication and recovery, and post-incident activity. Security incidents are logged in the AWS Guard Duty and internal ProjectEye solution and appropriately followed through the incident response lifecycle. The Incident Response Plan is tested on an annual basis or more frequently as needed. ESW defines a security incident as any irregular or suspicious event that might affect the security or availability of systems and data.

The Security Incident Response Team comprises management and employees representing infrastructure and product development and support. The SIRT also seeks support from other departments and external forensic professionals as needed.

Security incidents are detected through network devices, AWS alerts, and logs for suspicious events. Once the security incident is detected, the SIRT works quickly to analyze and validate each incident following a predefined process documenting each step taken. The initial analysis provides information to prioritize subsequent activities, such as containment of the incident and a deeper analysis of the effects of the incident. The security incident is logged in and followed through the incident response lifecycle.

During/after incident detection and analysis, the SIRT notifies appropriate internal employees and law enforcement as needed. If the incident/breach impacts sensitive or personal data, notice is provided to customers affected.

Post-mortem activities include holding a “lessons learned” meeting with all involved parties after a major incident, and optionally after lesser incidents as deemed necessary. This meeting seeks to review what occurred, what was done to intervene, and how well the intervention worked. The Incident Response Policy is updated as needed after each lesson learned session.

Backup and Recovery

ESW’s backup strategy includes snapshot images of volumes and databases performed daily and the full-system backups are performed weekly. ESW uses RDS snapshot backups for SQL databases. RDS backups are also used to archive and store database backups, which are encrypted during the backup process. In addition, the source code of the configuration management and infrastructure orchestration system is backed up so infrastructure and services can be restored quickly.

The disaster recovery strategy is predicated on a high availability scheme that has been established and configured for the DynamoDB system to reside at AWS in multiple availability zones. As part of the AWS S3 service offering, all data stored within AWS S3 includes cross-region replication which automatically replicates data across different AWS regions. In the event one zone is unavailable, complete copies of production systems are available in other AWS zones.

The Disaster Recovery and Business Continuity Policy outlines the disaster recovery and business continuity strategy in place for ESW operations located in AWS and production systems and data located at the separate AWS accounts.

The Disaster Recovery and Business Continuity Plan is tested on an annual basis. The test is conducted within a realistic environment that includes simulating conditions that are applicable in an actual emergency. Results of this test are reviewed, and updates are made to the plan/policy as necessary.

Risk Assessment

ESW recognizes the importance of risk management in properly managing customer data and providing high-quality, cost-effective services to its customers. The Chief Technology Officer (CTO) and Chief Information Officer (CIO) oversee the annual assessment of risk with respect to the IT processing environment and related application systems and services provided to users of the ESW systems.

ESW Company evaluates risks that may threaten the achievement of its system requirements and service commitments related to security and availability based on the Trust Service Criteria in *TSP Section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Documented policies and procedures are in place to guide personnel in identifying business objective risks. Upon assessment of the significance and likelihood of a particular risk, management considers how the risk should be managed, which involves judgment based on assumptions and analysis of costs to reduce the level of risk. Changes in technology, applicable laws and regulations, security threats, and risks are reviewed by ESW on a periodic basis, and existing control activities and Information Security policies are updated as a result.

Information Security management assesses security risks on an ongoing basis. This is accomplished through quarterly Risk Review Meetings with Security and Legal, in addition to regular activities such as reviewing and acting on security event logs/alerts, performing periodic vulnerability assessments, reviewing the information provided via anonymous whistleblower channels, and conducting a formal annual Risk Assessment.

The annual Enterprise Risk Assessment seeks to identify risks to the ESW System platforms and overall business. Risks are assessed from a qualitative perspective, risk treatment measures are documented, and controls are mapped appropriately, where necessary. After the Risk Assessment is completed, Information Security meets with Executive Management to present findings and receive feedback.

The SAFE Committee meets quarterly to review all outstanding risks and identify any new risks based on changes to the business, regulatory requirements, or vendor relationships.

Fraud Risk Assessment

Management considers the potential for fraud, which can occur in both financial and non-financial reporting when assessing risks to ESW's business objectives. Non-existent, insufficient, or ineffective controls provide an opportunity for fraud when combined with pressure or an incentive to commit fraud. Therefore, the potential for fraud is assessed on an annual basis as part of the formal Enterprise Risk Assessment.

Vendor Risk Assessment

ESW has a documented vendor risk management process in place, which includes performing due diligence prior to agreeing to services with new vendors or business partners. As part of this rigorous evaluation process, vendors are provided a compliance questionnaire, which assesses and seeks to identify security risks that may arise from sharing data or otherwise partnering with the organization. Data privacy risks are also evaluated, though the depth of the evaluation is largely dependent on the location of the organization. For example, US-based companies are questioned on where they store data, what compliance laws and regulations they are subject to, in which countries they do business, and their process to obtain explicit consent from data subjects.

On a periodic basis, management assesses the compliance status of critical vendors, subservice organizations, or business partners, communicates security incidents or issues as necessary, and terminates contracts in the event that security commitments are not met. Annually, at minimum, vendor risk is evaluated as a component of the Enterprise Risk Assessment and SOC audit reports of key subservice organizations are reviewed for appropriateness, including complementary user entity controls. Management requires all subservice organizations without a SOC report to fill out a questionnaire to evaluate risk

Customer Security Risk Evaluation

Once a customer is registered for the platform, the customer is provided with a compliance questionnaire to assess security risks, including data encryption methods, privileged access management, etc. The Privacy and Security team reviews the responses and reaches out to the customer to request remediation, where necessary. Upon successful remediation of identified gaps, the risk evaluation process is complete, and the customer can be given access to the ESW platform.

Information and Communication

ESW obtains relevant and quality information from internal and external sources, such as security monitoring tools, data imported via API, data processed via a high-performance messaging broker, and management assessments of risks to the production environment. Additionally, management has implemented various communication methods for employees and external parties to help ensure that communication occurs broadly and in all directions within the organization. These methods include but are not limited to, management meetings, documented job descriptions, policy distribution, and acknowledgments, change and incident management tickets, and documented policies and procedures that are formally documented and clearly communicated to all employees.

Internal Communication

ESW's information security policies are updated annually, at minimum, and are published to all employees internally via SharePoint. The Employee Handbook also contains a reference to security responsibilities, as well as disciplinary procedures for not adhering to security protocols within the organization. The Employee Handbook and security policies are acknowledged by all employees upon hire, and the security policies are acknowledged annually thereafter. Additionally, ESW requires all employees to sign confidentiality and non-solicitation agreements before starting work in the organization.

The security policies and responsibilities are reinforced through security and privacy awareness training, which occurs upon hire and annually thereafter. Additionally, event-driven security reminders/notifications are communicated as needed.

External Communication

ESW Company's security commitments are communicated to customers via an executed agreement or contract. Multiple communication channels are in place to allow customers to report security incidents, failures, concerns, or other complaints, including a web-based customer support ticketing system accessible from the ESW Company Support portal.

In the case of a confirmed data breach, ESW would notify customers within 48-72 hours or as required by contractual agreements and applicable local law. If a breach involves ESW Company's data, as opposed to customer data, ESW will notify the regulatory agencies within 72 hours or as required by applicable local law.

Various methods of communication are used to ensure that service commitments and system requirements are communicated and addressed in a timely manner. Email and Slack are used to communicate time-sensitive messages. Executive leadership, manager, and staff meetings are held on a periodic basis and as needed. An All-Hands Meeting, where company objectives and performance is discussed, is held on a quarterly basis with all employees.

Significant System and Control Changes

The IT environment has been stable throughout the period and there have been no significant changes to the system. The description does not omit or distort information relevant to ESW's system. ESW acknowledges the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

4 Monitoring

The CISO monitors the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to determine if objectives are achieved, identify any new risks that develop, and implement appropriate measures to address those risks. ESW adopts a proactive approach to the monitoring of application and network security to ensure that any issues or risks are identified and addressed as soon as possible.

Separate Evaluations

Evaluations of internal control vary in scope and frequency, depending on the significance of risks being managed and the importance of the controls in reducing risks. Evaluations often take the form of informal self-assessments, where personnel responsible for a particular function determine the effectiveness of controls for their activities.

Security reviews and vulnerability assessments are performed or coordinated by Information Security personnel periodically to identify threats and assess their potential impacts on system security. Any detected security vulnerabilities are investigated and documented through remediation.

Subservice Organizations

A subservice organization is used to deliver products and services that ESW Company relies on to serve its customers and clients.

Amazon Web Services (AWS)
ESW uses **Amazon Web Services (AWS)** as the cloud hosting provider for the ESW Product Platforms. The following Complementary Sub service Organization Controls (CSOCs) are expected to be operating effectively at AWS, alone or in combination with controls at ESW, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Control
6.1, 6.2, 6.3, 6.5, 6.6	AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.
6.4, 6.5	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.
6.7	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices.
A 1.1	AWS is responsible for ensuring capacity demand controls are in place to meet availability commitments and requirements.
A 1.2	AWS is responsible for ensuring environmental protection controls are in place to meet availability commitments and requirements.
A 1.3	AWS is responsible for managing the redundant infrastructure used and configured by ESW for recovery operations.

ESW Management receives and reviews the AWS SOC 2 Type 2 report on an annual basis. Any deficiencies identified in a subservice organization's SOC 2 report are analyzed for relevance to and effect on ESW's organization and its users. As part of the review:

- Management confirms that the CSOCs listed above are covered within the scope of AWS' SOC 2 Type 2 report and are found to be operating effectively during the audit period.
- Management determines that the Complementary User Entity Controls (CUECs) identified in AWS' SOC 2 Type 2 report are included in the scope of this SOC 2 report as controls that are tested by the service auditor.

In addition, through its daily operational activities, management monitors the services performed by AWS to ensure that operations and controls expected to be implemented are functioning effectively.

5 Complementary User Entity Controls and Responsibilities

The control activities performed by ESW were designed with the understanding that certain user organization controls would be implemented by each customer. Each customer's internal control structure must be evaluated in conjunction with ESW's controls, policies and procedures described in this report. The Complementary User Entity Controls (CUECs) below are the minimum controls that customers must have in operation to complement the controls of the ESW product system and should not be regarded as a comprehensive list of all controls that should be employed by customers.

Complementary User Entity Controls	Related Applicable Criteria
Users are responsible for adhering to all regulatory compliance issues when they are associated with ESW in a service agreement.	2.3
Users are responsible for reviewing and approving the terms and conditions stated in service agreements with ESW.	2.3
External users are responsible for resetting the initial password created to access the ESW product platform.	6.1
Users are responsible for selecting and using strong passwords in accordance with ESW Product's password requirements enforced on the application.	6.1, 6.2
Users are responsible for ensuring user access to reports and other information generated from ESW is restricted based on business needs.	6.1, 6.3

Complementary User Entity Controls	Related Applicable Criteria
Users are responsible for ensuring user-owned or managed applications, platforms, databases, and network devices that may process or store data derived from ESW are logically and physically secured.	6.1, 6.3
Users of ESW-hosted applications are responsible for maintaining appropriate IT General Computer Controls and Application Controls.	6.1, 6.3

6 Non-Applicable Trust Services Criteria

Non-Applicable TS Criteria	Security Trust Principle	Message Broadcast's Rationale
1.2.1	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	ESW Operations, LLC does not have a Board of Directors.

SECTION FOUR

Trust Services Criteria, Related Controls, and Tests of Controls

TRUST SERVICES CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

1 Scope, Purpose, and Objectives of the Report

The scope of CyberGuard Compliance, LLP's ("CGC") procedures was based on the AICPA and trust services criteria relevant to Security and Availability as they relate to the system and the design and operating effectiveness of the applicable controls. This report, when combined with an understanding and assessment of the internal controls at user organizations, is intended to meet the needs of a broad range of users that need information and assurance about the controls at ESW that affect the Security and Availability criteria of the system. Stakeholders who may need this report are: management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls.

APPLICABLE TRUST SERVICES CRITERIA

The applicable trust services criteria and related controls presented in Section 4, "Trust Services Criteria, Related Controls, and Tests of Controls," are an integral part of ESW's system description throughout the period October 1, 2023 to September 30, 2024.

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:

i. information during its collection or creation, use processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of ESW 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.

Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by ESW's systems, as well as the products or services provided to its customers. While the availability objective does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Our examination was restricted to the Trust Services Criteria specified above and related control procedures specified in Section 4. It is the stakeholders' responsibility to evaluate this information in relation to the controls in place at each user organization.

2 Tests of Operating Effectiveness

Our tests of the operating effectiveness of controls were designed to cover a representative number of transactions for the period October 1, 2023 to September 30, 2024 for each of the trust services criteria listed in Section 4, which are designed to achieve the specific criteria. Tests of design and operating effectiveness were based off the criteria and illustrative controls within each trust services criteria.

Type of Test	General Description of Test
Inquiry or corroborative inquiry	Inquired of appropriate personnel to ascertain compliance with controls
Observation	Observed application of specific controls
Inspection	Obtained and examined documents and reports indicating performance of the controls
Re-Performed	Re-performed application of the controls

In addition, as required by paragraph .35 of ATC Section 205, Assertion-Based Examination Engagements (AICPA, *Professional Standards*), and paragraph .30 of ATC Section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

This assessment was performed virtually using Information and Communication Technology (ICT).

3 Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), CGC performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1) Inspect the source of the IPE
2) Inspect the query, script, or parameters used to generate the IPE
3) Tie data between the IPE and the source
4) Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity

In addition to the above, procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), CGC inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria for Security

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
1.1.1	The Company has a formalized Code of Conduct, which demonstrates the importance of integrity and ethical values. The Code of Conduct is included in the Employee Handbook, which is available to employees via the intranet.	**Inspection:** Obtained and reviewed the Code of Conduct and the screenshot of the location of the policies. Verified the Code of Conduct was included in the Employee Handbook, which was available to employees via the intranet.	No exceptions noted.
1.1.2	New employees sign a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the policy acknowledgement report for the sampled employees hired during the audit period. Verified new employees signed a statement signifying that they have received, read, understood, and will follow the Company Code of Conduct and all internal policies.	No exceptions noted.
1.1.3	Employees receive a formal performance review annually.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received a formal performance review annually.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
1.1.4	The Company has established disciplinary policies for employees who violate security policies/acceptable use policies/company policies.	**Inspection:** Obtained and reviewed the Sanctions Policy. Verified the policy contained disciplinary procedures for employees who violate security, acceptable use, and company policies.	No exceptions noted.
1.2	COSO Principle 2: The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
Not applicable. See Section 3 for details.			
1.3	COSO Principle 3: Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
1.3.1	Reporting relationships and organizational structures are reviewed annually by senior management as part of organizational planning, and are adjusted as needed based on changing Company commitments and requirements.	**Inspection:** Obtained and reviewed the organizational chart and management's review. Verified reporting relationships and organizational structures were reviewed annually by senior management as part of organizational planning, and were adjusted as needed based on changing Company commitments and requirements.	No exceptions noted.
1.3.2	Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the job descriptions for the sampled job roles during the audit period. Verified roles and responsibilities were defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
1.4.1	Employees receive a formal performance review annually.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received a formal performance review annually.	No exceptions noted.
1.4.2	Background checks are performed prior to personnel being hired by the Company.	**Inspection:** Obtained and reviewed the background check reports for the sampled employees hired during the audit period. Verified personnel passed a criminal background check before they were hired by the Company.	No exceptions noted.
1.4.3	The experience and training of candidates for employment are verified before they assume the responsibilities of their position.	**Inspection:** Obtained and reviewed the employee interview results for the sampled employees hired during the audit period. Verified the experience and training of candidates for employment was verified before they assumed the responsibilities of their position.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.4.4	Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the job descriptions for the sampled job roles during the audit period. Verified roles and responsibilities were defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.	No exceptions noted.
1.4.5	Personnel are required to attend annual security awareness training.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the security awareness training report for the sampled active employees during the audit period. Verified personnel attended annual security awareness training.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
1.5.1	Documented policies are in place, reviewed annually and are available to all applicable personnel. These policies include the Employee Handbook, Disciplinary Policy, Risk Management Policy, Data Retention and Disposal Policy, Encryption Management Policy, Change Management Policy, Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies. Verified documented internal control policies were updated annually and were available to appropriate employees and contractors. These policies included the Employee Handbook, Disciplinary Policy, Risk Management Policy, Data Retention and Disposal Policy, Encryption Management Policy, Change Management Policy, Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
1.5.2	The Chief Information Security Officer is responsible for maintaining the Company's security practices and commitments.	**Inspection:** Obtained and reviewed the Chief Information Security Officer's job description. Verified the Information Security Officer was responsible for maintaining the Company's security practices and commitments.	No exceptions noted.
1.5.3	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

1.0 CONTROL ENVIRONMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
1.5.4	Personnel are required to attend annual security awareness training.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the security awareness training report for the sampled active employees during the audit period. Verified personnel attended annual security awareness training.	No exceptions noted.
1.5.5	Employees receive a formal performance review annually.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the performance reviews for the sampled active employees during the audit period. Verified employees received a formal performance review annually.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
2.1.1	The Company reviews its data flow diagram annually.	**Inspection:** Obtained and reviewed the architecture documents. Verified the Company reviewed its data flow diagram annually.	No exceptions noted.
2.1.2	The Data Classification Policy details roles and responsibilities, data classification model, data sensitivity levels, and a security requirements matrix.	**Inspection:** Obtained and reviewed the Data Classification Policy. Verified the Data Classification Policy detailed roles and responsibilities, data classification model, data sensitivity levels, and a security requirements matrix.	No exceptions noted.
2.1.3	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The inventory identifies the classification, location, owners, and custodians. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The inventory identified the classification, location, owners, and custodians. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
2.1.4	Weekly, engineering meetings are held to discuss client related changes.	**Inspection:** Obtained and reviewed the weekly engineering meeting minutes for the sampled weeks during the audit period. Verified engineering meetings are held to discuss client related changes weekly.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
2.2.1	The Chief Information Security Officer is responsible for maintaining the Company's security practices and commitments.	**Inspection:** Obtained and reviewed the Chief Information Security Officer's job description. Verified the Information Security Officer was responsible for maintaining the Company's security practices and commitments.	No exceptions noted.
2.2.2	Documented policies are in place, reviewed annually and are available to all applicable personnel. These policies include the Employee Handbook, Disciplinary Policy, Risk Management Policy, Data Retention and Disposal Policy, Encryption Management Policy, Change Management Policy, Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies. Verified documented internal control policies were updated annually and were available to appropriate employees and contractors. These policies included the Employee Handbook, Disciplinary Policy, Risk Management Policy, Data Retention and Disposal Policy, Encryption Management Policy, Change Management Policy, Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
2.2.3	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.2.4	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Security Incident Response and Breach Notification Manual and the most recent incident response training session detail report. Verified a comprehensive Incident Response Plan was communicated to staff and regularly updated. Additionally verified incident response training was held annually.	No exceptions noted.
2.2.5	Changes made to systems are communicated to appropriate users.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified changes made to systems were communicated to appropriate users.	No exceptions noted.
2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
2.3.1	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Security Incident Response and Breach Notification Manual and the most recent incident response training session detail report. Verified a comprehensive Incident Response Plan was communicated to staff and regularly updated. Additionally verified incident response training was held annually.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
2.3.2	Company policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it is encrypted.	**Inspection:** Obtained and reviewed the Data Transfer Policy and the Encryption Management Policy. Verified company policies prohibited the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it was encrypted.	No exceptions noted.
2.3.3	Applicable Company security and availability commitments regarding the system are included in the Master Service Agreement and/or customer-specific Service Level Agreements. Relevant updates and changes to agreements are communicated to external parties as needed.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the Master Service Agreements for the sampled customers during the audit period. Verified applicable Company security and availability commitments regarding the system are included in the Master Service Agreement and/or customer-specific Service Level Agreements. Relevant updates and changes to agreements were communicated to external parties as needed.	No exceptions noted.

2.0 INFORMATION AND COMMUNICATION			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
2.3.4	Customer responsibilities, which may include the responsibility and process for reporting operational failures, incidents, problems, concerns, and complaints, are described in the Master Service Agreements, Statements of Work, or Service Level Agreements. Relevant updates and changes to agreements are communicated to external parties as needed.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the Master Service Agreements for the sampled customers during the audit period. Verified customer responsibilities, which included the responsibility and process for reporting operational failures, incidents, problems, concerns, and complaints, were described in the Master Service Agreements, Statements of Work, or Service Level Agreements. Relevant updates and changes to agreements were communicated to external parties as needed.	No exceptions noted.
2.3.5	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
3.1.1	A formally documented Information Risk Management Policy is maintained and reviewed annually.	**Inspection:** Obtained and reviewed the Risk Management Policy and Procedure. Verified a formally documented Information Risk Management Policy was maintained and reviewed annually.	No exceptions noted.
3.1.2	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.
3.1.3	Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.
3.1.4	The SAFE Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the risk review meeting minutes for the sampled quarters during the audit period. Verified the SAFE Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affected the selection and development of control activities.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
3.2.1	Business Continuity and Disaster Recovery Plans are in place to identify the criticality of information assets.	**Inspection:** Obtained and reviewed the Business Continuity and Disaster Recovery Plan. Verified Business Continuity and Disaster Recovery Plans were in place to identify the criticality of information assets.	No exceptions noted.
3.2.2	Internal vulnerability and external vulnerability scans are performed semi-annually. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the sampled internal and external vulnerability scan reports and the vulnerability monitoring dashboard. Verified internal and external vulnerability scans were performed semi-annually. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
3.2.3	Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.
3.2.4	The Company maintains a formal Vendor Risk Management process that assesses the potential threats and vulnerabilities from vendors providing goods and services. The Company assesses, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	**Inspection:** Obtained and reviewed the Vendor Management Policy. Verified the Company maintained a formal Vendor Risk Management process that assessed the potential threats and vulnerabilities from vendors providing goods and services.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.2.5	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.
3.2.6	The SAFE Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the risk review meeting minutes for the sampled quarters during the audit period. Verified the SAFE Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affected the selection and development of control activities.	No exceptions noted.
3.2.7	Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.
3.2.8	Unremediated risks are assessed by Management as needed. Remediation activities are documented and resolved in a timely manner.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified unremediated risks were assessed by Management as needed. Remediation activities were documented and resolved in a timely manner.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
3.3.1	An enterprise risk assessment is performed annually and considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified an enterprise risk assessment was performed annually and considered fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	No exceptions noted.
3.3.2	The enterprise risk assessment considers how management and other personnel might engage in or justify inappropriate actions.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the enterprise risk assessment considered how management and other personnel might engage in or justify inappropriate actions.	No exceptions noted.
3.3.3	The enterprise risk assessment considers threats and vulnerabilities that arise specifically from the use of IT and access to information.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the enterprise risk assessment considered threats and vulnerabilities that arise specifically from the use of IT and access to information.	No exceptions noted.
3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
3.4.1	The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the risk identification process considered changes to the regulatory, economic, and physical environment in which the Company operates.	No exceptions noted.

3.0 RISK ASSESSMENT			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
3.4.2	The risk identification process considers changes in the Company’s systems and in the technology environment.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the risk identification process considered changes in the Company’s systems and in the technology environment.	No exceptions noted.
3.4.3	The risk identification process considers changes in vendor and business partner relationships.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the risk identification process considered changes in vendor and business partner relationships.	No exceptions noted.
3.4.4	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.
3.4.5	The SAFE Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the risk review meeting minutes for the sampled quarters during the audit period. Verified the SAFE Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affected the selection and development of control activities.	No exceptions noted.
3.4.6	Compliance objectives include any external laws or regulations with which the Company must comply.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified compliance objectives included any external laws or regulations with which the Company must comply.	No exceptions noted.

4.0 MONITORING ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
4.1.1	Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.
4.1.2	Internal vulnerability and external vulnerability scans are performed semi-annually. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the sampled internal and external vulnerability scan reports and the vulnerability monitoring dashboard. Verified internal and external vulnerability scans were performed semi-annually. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
4.1.3	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the system configuration monitoring system. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards with the assistance of automated software tools.	No exceptions noted.
4.1.4	Errors identified from job monitoring are sent to the SaaS Ops Team for tracking.	**Inspection:** Obtained and reviewed the error monitoring system. Verified errors identified from job monitoring were sent to the SaaS Ops Team for tracking.	No exceptions noted.

4.0 MONITORING ACTIVITIES			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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.		
4.2.1	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.
4.2.2	Unremediated risks are assessed by Management as needed. Remediation activities are documented and resolved in a timely manner.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified unremediated risks were assessed by Management as needed. Remediation activities were documented and resolved in a timely manner.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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.		
5.1.1	The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the risk identification process considered changes to the regulatory, economic, and physical environment in which the Company operates.	No exceptions noted.
5.1.2	The risk identification process considers changes in the Company's systems and in the technology environment.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the risk identification process considered changes in the Company's systems and in the technology environment.	No exceptions noted.
5.1.3	The risk identification process considers changes in vendor and business partner relationships.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified the risk identification process considered changes in vendor and business partner relationships.	No exceptions noted.
5.1.4	Control activities are mapped to the Company's risk assessment to ensure that risk responses address and mitigate risks.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified control activities were mapped to the Company's risk assessment to ensure that risk responses address and mitigate risks.	No exceptions noted.
5.1.5	A formal risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.	**Inspection:** Reviewed the enterprise risk assessment through ICT methods. Verified a formal risk assessment was performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts were identified.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.1.6	The SAFE Committee meets on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	**Inspection:** Obtained and reviewed the risk review meeting minutes for the sampled quarters during the audit period. Verified the SAFE Committee met on a quarterly basis to discuss matters/risks pertinent to security operations and the business and considered how the environment, complexity, nature, and scope of its operations affected the selection and development of control activities.	No exceptions noted.
5.2	COSO Principle 11: The entity selects and develops general control activities over technology to support the achievement of objectives.		
5.2.1	Documented configuration standards are reviewed annually, at minimum, and when significant changes are made or integral system components are added.	**Inspection:** Obtained and reviewed the Server Hardening Procedures. Verified documented configuration standards were reviewed annually, at minimum, and when significant changes were made or integral system components were added.	No exceptions noted.
5.2.2	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the User Access Procedure. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
5.2.3	The Company maintains recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	**Inspection:** Obtained and reviewed the Backup and Recovery Policy. Verified the Company maintained recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	No exceptions noted.
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.		
5.3.1	Documented policies are in place, reviewed annually and are available to all applicable personnel. These policies include the Employee Handbook, Disciplinary Policy, Risk Management Policy, Data Retention and Disposal Policy, Encryption Management Policy, Change Management Policy, Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	**Inspection:** Obtained and reviewed the internal control policies. Verified documented internal control policies were updated annually and were available to appropriate employees and contractors. These policies included the Employee Handbook, Disciplinary Policy, Risk Management Policy, Data Retention and Disposal Policy, Encryption Management Policy, Change Management Policy, Information Security Policy, Data Classification Policy, Incident Response Policy, Vendor Risk Management Policy, and Business Continuity and Disaster Recovery Policy.	No exceptions noted.
5.3.2	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the User Access Procedure. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

5.0 CONTROL ACTIVITIES			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
5.3.3	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Response Manual. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
5.3.4	New employees sign a statement signifying that they have received, read, understand, and will follow the Company Code of Conduct and all internal policies.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the policy acknowledgement report for the sampled employees hired during the audit period. Verified new employees signed a statement signifying that they have received, read, understood, and will follow the Company Code of Conduct and all internal policies.	No exceptions noted.
5.3.5	The list of internal controls is communicated to process owners, reviewed, and updated annually.	**Inspection:** Obtained and reviewed the internal control assessment. Verified the list of internal controls was communicated to process owners, reviewed, and updated annually.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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.		
6.1.1	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The inventory identifies the classification, location, owners, and custodians. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The inventory identified the classification, location, owners, and custodians. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
6.1.2	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	No exceptions noted.
6.1.3	Users are required to authenticate via unique user account ID and password before being granted access to in-scope networks, systems, and applications.	**Inspection:** Obtained and reviewed the user listing and login portal. Verified users were required to authenticate via unique user account ID and password before being granted access to in-scope networks, systems, and applications.	No exceptions noted.
6.1.4	Administrator access is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the listing of administrators and reconciled with the employee listing. Verified administrator access was limited to only authorized personnel.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
6.1.5	Administrators must authenticate via unique ID and password before being granted access to in-scope networks, systems, and applications.	**Inspection:** Obtained and reviewed the administrator user listing and reconciled with the employee listing. Verified administrators must authenticate via unique ID and password before being granted access to in-scope networks, systems, and applications.	No exceptions noted.
6.1.6	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the user access requests for the sampled employees hired during the audit period. Verified new user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) was used to support segregation of incompatible functions.	No exceptions noted.
6.1.7	Modified user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of access modifications during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the User, Vendor and Customer Access Policy, and verified modified user access to the network and in-scope applications is to be authorized by appropriate personnel and granted based on job role via the access provisioning process.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.8	The Company has documented policies and procedures on the use of cryptographic controls for protection of information.	**Inspection:** Obtained and reviewed the Encryption Management Policy. Verified the Company had documented policies and procedures on the use of cryptographic controls for protection of information.	No exceptions noted.
6.1.9	The production network domain is configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	**Inspection:** Obtained and reviewed the domain password configuration. Verified the production network domain was configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.1.10	In-scope applications are configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	**Inspection:** Obtained and reviewed the password configurations for the in-scope systems noting one system did not have a default password configuration and several other in-scope systems only required a minimum password length. Therefore, the auditors were unable to verify the in-scope applications are configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Account Lockout for excessive invalid login attempts • Strong password complexity	***Exception noted. See Section 5 for further details.***
6.1.11	The system automatically logs out users after a defined period of inactivity.	**Inspection:** Obtained and reviewed the system timeout configuration. Verified the system automatically logged out users after a defined period of inactivity.	No exceptions noted.
6.1.12	Separate environments are used for development, testing, and production.	**Inspection:** Obtained and reviewed the environment listings. Verified separate environments were used for development, testing, and production.	No exceptions noted.
6.1.13	Developers do not have the ability to migrate changes to production.	**Inspection:** Obtained and reviewed the source code deployment configuration. Verified developers did not have the ability to migrate changes to production.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
6.1.14	Confidential data files are encrypted prior to backup.	**Inspection:** Obtained and reviewed the database encryption configuration. Verified confidential data files were encrypted prior to backup.	No exceptions noted.
6.1.15	Access to add or delete jobs to / from the job scheduler is restricted to personnel commensurate with their job role.	**Inspection:** Obtained and reviewed the administrator listing and reconciled with the employee list. Verified access to add or delete jobs to / from the job scheduler was restricted to personnel commensurate with their job role.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.			
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.		
6.2.1	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the User Access Procedure. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
6.2.2	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the user access requests for the sampled employees hired during the audit period. Verified New and modified user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) was used to support segregation of incompatible functions.	No exceptions noted.
6.2.3	Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled terminated employees during the audit period. Verified IT terminated logical access within 24 hours of notification.	No exceptions noted.
6.2.4	A user access review of network and application accounts, and associated permissions, is performed semi-annually to ensure appropriate logical access is maintained.	**Inspection:** Obtained and reviewed the user access reviews performed during the audit period. Verified a user access review of network and application accounts, and associated permissions, was performed semi-annually to ensure appropriate logical access was maintained.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
6.2.5	Management performs a review of network and application administrator access quarterly to ensure that appropriate privileged access is restricted.	**Inspection:** Obtained and reviewed the administrator access reviews performed for the sampled quarters during the audit period. Verified a user access review of network and application accounts, and associated permissions, was performed quarterly to ensure appropriate logical access was maintained.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.			
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.		
6.3.1	Policies and procedures define requirements for granting, provisioning, and revoking access to data and systems. The assignments are role-based and are defined by management.	**Inspection:** Obtained and reviewed the User Access Procedure. Verified policies and procedures defined requirements for granting, provisioning, and revoking access to data and systems. The assignments were role-based and were defined by management.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
6.3.2	New user access to the network and in-scope applications is authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) is used to support segregation of incompatible functions.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the user access requests for the sampled employees hired during the audit period. Verified New and modified user access to the network and in-scope applications was authorized by appropriate personnel and granted based on job role via the access provisioning process. Role-Based Access Control (RBAC) was used to support segregation of incompatible functions.	No exceptions noted.
6.3.3	Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the termination tickets for the sampled terminated employees during the audit period. Verified IT terminated logical access within 24 hours of notification.	No exceptions noted.
6.3.4	The ability to modify the AWS configuration or ruleset is restricted to personnel commensurate with their job role.	**Inspection:** Obtained and reviewed the administrator listing and reconciled with the employee list. Verified the ability to modify the AWS configuration or ruleset was restricted to personnel commensurate with their job role.	No exceptions noted.
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.			

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.			
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.		
6.5.1	The Data Asset Inventory contains the data assets that are key to the safe and continued operation of the business. The inventory identifies the classification, location, owners, and custodians. The Data Asset Inventory is reviewed and updated annually.	**Inspection:** Obtained and reviewed the Data Asset Inventory. Verified the Data Asset Inventory contained the data assets that were key to the safe and continued operation of the business. The inventory identified the classification, location, owners, and custodians. The Data Asset Inventory was reviewed and updated annually.	No exceptions noted.
6.5.2	Formal data retention and disposal procedures are in place to guide the secure disposal of data that has been identified for destruction in a manner that prevents loss, theft, misuse, or unauthorized access.	**Inspection:** Obtained and reviewed the data retention and disposal procedures. Verified formal data retention and disposal procedures were in place to guide the secure disposal of data that had been identified for destruction in a manner that prevented loss, theft, misuse, or unauthorized access.	No exceptions noted.
6.5.3	Policies and procedures define requirements for employee laptop encryption in the event they are lost or stolen.	**Inspection:** Obtained and reviewed the Encryption Management Policy. Verified policies and procedures defined requirements for employee laptop encryption in the event they are lost or stolen.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services. AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.			
6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
6.6.1	Administrator access is limited to only authorized personnel.	**Inspection:** Obtained and reviewed the listing of administrators and reconciled with the employee listing. Verified administrator access was limited to only authorized personnel.	No exceptions noted.
6.6.2	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	No exceptions noted.
6.6.3	SSH keys are used to access all storage nodes.	**Inspection:** Obtained and reviewed the SSH configuration. Verified SSH keys were used to access all storage nodes.	No exceptions noted.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
6.6.4	Firewalls are in place to protect production systems and are configured to restrict unnecessary ports, protocols, and services. Logs are monitored to detect any potential security vulnerabilities or unauthorized access attempts.	**Inspection:** Obtained and reviewed the security group configuration, and security group logs. Verified firewalls were in place to protect production systems and were configured to restrict unnecessary ports, protocols, and services. Logs were monitored to detect any potential security vulnerabilities or unauthorized access attempts.	No exceptions noted.
6.6.5	The Company uses Transport Layer Security (TLS 1.0 or higher) for transmitting sensitive data over public networks.	**Inspection:** Obtained and reviewed the Transport Layer Security (TLS) server reports. Verified the Company utilized TLS for transmitting sensitive data over public networks.	No exceptions noted.
6.6.6	An Intrusion Detection and Prevention System is configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	**Inspection:** Obtained and reviewed the Intrusion Detection and Prevention System configuration and monitoring dashboard. Verified an Intrusion Detection and Prevention System was configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	No exceptions noted.
6.6.7	Policies and procedures define requirements for employee laptop encryption in the event they are lost or stolen.	**Inspection:** Obtained and reviewed the Encryption Management Policy. Verified policies and procedures defined requirements for employee laptop encryption in the event they are lost or stolen.	No exceptions noted.

AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services.

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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.		
6.7.1	The Company has documented policies and procedures on the use of cryptographic controls for protection of information.	**Inspection:** Obtained and reviewed the Encryption Management Policy. Verified the Company had documented policies and procedures on the use of cryptographic controls for protection of information.	No exceptions noted.
6.7.2	Remote access to production systems is permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	**Inspection:** Obtained and reviewed the VPN configuration. Verified remote access to production systems was permitted using multi-factor authentication over an encrypted tunnel (VPN) for authorized employees, contractors, and third parties.	No exceptions noted.
6.7.3	The Company uses Transport Layer Security (TLS 1.0 or higher) for transmitting sensitive data over public networks.	**Inspection:** Obtained and reviewed the Transport Layer Security (TLS) server reports. Verified the Company utilized TLS for transmitting sensitive data over public networks.	No exceptions noted.
6.7.4	Policies and procedures define requirements for employee laptop encryption in the event they are lost or stolen.	**Inspection:** Obtained and reviewed the Encryption Management Policy. Verified policies and procedures defined requirements for employee laptop encryption in the event they are lost or stolen.	No exceptions noted.
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices.			

6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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.		
6.8.1	The Company has a documented Change Management Policy that addresses changes to system components, including those that may affect system security. Such changes require approval from IT management, or an authorized delegate, before implementation. The policy is reviewed annually.	**Inspection:** Obtained and reviewed the Change Management Policy. Verified the Company had a documented Change Management Policy that addressed changes to system components, including those that may affect system security. Such changes required approval from IT management, or an authorized delegate, before implementation. The policy was reviewed annually.	No exceptions noted.
6.8.2	System and configuration management tools are used to maintain an inventory of installed applications and software and to monitor patch status. These tools log and alert IT of software installation or attempted software installation.	**Inspection:** Obtained and reviewed screenshots of the system management tool. Verified system and configuration management tools were used to maintain an inventory of installed applications and software and to monitor patch status. these tools logged and alerted IT of software installation or attempted software installation.	No exceptions noted.
6.8.3	Anti-virus software is installed on all servers and workstations. Updates are pushed to the nodes as new updates and signatures become available.	**Inspection:** Obtained and reviewed the anti-virus installation listing and configuration. Verified anti-virus software was installed on all servers and workstations. Updates were pushed to the nodes as new updates and signatures become available.	No exceptions noted.
6.8.4	Separate environments are used for development, testing, and production.	**Inspection:** Obtained and reviewed the environment listings. Verified separate environments were used for development, testing, and production.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
7.1.1	An enterprise monitoring tool is in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts are sent to security personnel.	**Inspection:** Obtained and reviewed screenshots of the system monitoring dashboard and alert configuration. Verified an enterprise monitoring tool was in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts were sent to security personnel.	No exceptions noted.
7.1.2	Internal vulnerability and external vulnerability scans are performed semi-annually. Their frequency is adjusted as needed to meet ongoing and changing commitments and requirements.	**Inspection:** Obtained and reviewed the sampled internal and external vulnerability scan reports and the vulnerability monitoring dashboard. Verified internal and external vulnerability scans were performed semi-annually. Their frequency was adjusted as needed to meet ongoing and changing commitments and requirements.	No exceptions noted.
7.1.3	Penetration tests of the key systems are performed at least annually.	**Inspection:** Obtained and reviewed the penetration test report. Verified penetration tests of the key systems were performed at least annually.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.1.4	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the system configuration monitoring system. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards with the assistance of automated software tools.	No exceptions noted.
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.		
7.2.1	External parties are provided with instructions for communicating potential security breaches to the Company.	**Inspection:** Obtained and reviewed the Master Service Agreements for the sampled customers during the audit period. Verified external parties were provided with instructions for communicating potential security breaches to the Company.	No exceptions noted.
7.2.2	The technical security configuration of information systems and network components (e.g., firewalls, routers, switches) is reviewed for compliance with the configuration standards manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually, at minimum.	**Inspection:** Obtained and reviewed the system configuration monitoring system. Verified the technical security configuration of information systems and network components (e.g., firewalls, routers, switches) was reviewed for compliance with the configuration standards with the assistance of automated software tools.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.2.3	An Intrusion Detection and Prevention System is configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	**Inspection:** Obtained and reviewed the Intrusion Detection and Prevention System configuration and monitoring dashboard. Verified an Intrusion Detection and Prevention System was configured to continuously monitor and analyze network traffic and system activity, and log and prevent malicious activity.	No exceptions noted.
7.2.4	Detected and reported security events are logged in a ticketing system, evaluated, classified, and tracked through to resolution.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the incident tickets for the sampled security events during the audit period. Verified detected and reported security events were logged in a ticketing system, evaluated, classified, and tracked through to resolution.	No exceptions noted.
7.2.5	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Response Manual. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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.		
7.3.1	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Response Manual. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.3.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Security Incident Response and Breach Notification Manual and the most recent incident response training session detail report. Verified a comprehensive Incident Response Plan was communicated to staff and regularly updated. Additionally verified incident response training was held annually.	No exceptions noted.
7.3.3	Detected and reported security events are logged in a ticketing system, evaluated, classified, and tracked through to resolution.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the incident tickets for the sampled security events during the audit period. Verified detected and reported security events were logged in a ticketing system, evaluated, classified, and tracked through to resolution.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
7.3.4	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Security Incident Response and Breach Policy, and verified management is to perform an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
7.3.5	The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inquiry and Inspection:** Inquired with Management and inspected the Business Continuity Plan and determined the plan was not tested during the audit period. Therefore, we were unable to verify The Business Continuity and Disaster Recovery Plan was tested annually using scenarios based on threat likelihood and magnitude and lack of availability of key personnel and systems.	***Exception noted. See Section 5 for further details.***

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
7.4.1	A formal Incident Management process is documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	**Inspection:** Obtained and reviewed the Incident Response Manual. Verified a formal Incident Management process was documented to define protocols for reporting potential security events, procedures for evaluating detected/reported security events, roles and responsibilities for managing security events, and escalation criteria to determine when to enact the Incident Response Plan.	No exceptions noted.
7.4.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Security Incident Response and Breach Notification Manual and the most recent incident response training session detail report. Verified a comprehensive Incident Response Plan was communicated to staff and regularly updated. Additionally verified incident response training was held annually.	No exceptions noted.

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.4.3	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Security Incident Response and Breach Policy, and verified management is to perform an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
7.5.1	The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inquiry and Inspection:** Inquired of Management and inspected the Business Continuity Plan and determined the plan was not tested during the audit period. Therefore, we were unable to verify The Business Continuity and Disaster Recovery Plan was tested annually using scenarios based on threat likelihood and magnitude and lack of availability of key personnel and systems.	***Exception noted. See Section 5 for further details.***

7.0 SYSTEM OPERATIONS			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
7.5.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Security Incident Response and Breach Notification Manual and the most recent incident response training session detail report. Verified a comprehensive Incident Response Plan was communicated to staff and regularly updated. Additionally verified incident response training was held annually.	No exceptions noted.
7.5.3	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Security Incident Response and Breach Policy, and verified management is to perform an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.

8.0 CHANGE MANAGEMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
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.		
8.1.1	The Company has adopted a formal Systems Development Life Cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of information systems and related technology. The SDLC considers Security requirements.	**Inspection:** Obtained and reviewed the Software Development Lifecycle Policy. Verified the Company has adopted a formal Systems Development Life Cycle (SDLC) methodology that governed the development, acquisition, implementation, and maintenance of information systems and related technology. The SDLC considered Security requirements.	No exceptions noted.
8.1.2	The Company has a documented Change Management Policy that addresses changes to system components, including those that may affect system security. Such changes require approval from IT management, or an authorized delegate, before implementation. The policy is reviewed annually.	**Inspection:** Obtained and reviewed the Change Management Policy. Verified the Company had a documented Change Management Policy that addressed changes to system components, including those that may affect system security. Such changes required approval from IT management, or an authorized delegate, before implementation. The policy was reviewed annually.	No exceptions noted.
8.1.3	System changes are documented, tested, and approved prior to migrating the change to production as part of the change management process.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified system changes were documented, tested, and approved prior to migrating the change to production as part of the change management process.	No exceptions noted.

8.0 CHANGE MANAGEMENT			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
8.1.4	Emergency changes are documented, authorized, tested, and approved following the Change Management Policy.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled emergency system changes during the audit period. Verified emergency changes were documented, authorized, tested, and approved following the Change Management Policy.	No exceptions noted.
8.1.5	Changes made to systems are communicated to appropriate users.	**Observation and Inspection:** Witnessed the generation of the sampled population through ICT methods. Obtained and reviewed the change tickets for the sampled system changes during the audit period. Verified changes made to systems were communicated to appropriate users.	No exceptions noted.
8.1.6	Vendor security patches are evaluated, and critical patches are applied to key systems and applications within 30 days of release.	**Inspection:** Evidence of patch evaluation and application was unavailable for review. Therefore, the auditors could not determine whether critical patches were consistently evaluated and applied to key systems and applications within the 30-day window.	***Exception noted. See Section 5 for further details.***
8.1.7	Version control software is utilized to restrict access to application source code and provide rollback capabilities.	**Inspection:** Obtained and reviewed the source code user listing and rollback configuration. Verified version control software was utilized to restrict access to application source code and provide rollback capabilities.	No exceptions noted.

9.0 RISK MITIGATION			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
9.1.1	A formally documented Information Risk Management Policy is maintained and reviewed annually.	**Inspection:** Obtained and reviewed the Risk Management Policy and Procedure. Verified a formally documented Information Risk Management Policy was maintained and reviewed annually.	No exceptions noted.
9.1.2	An insurance policy is in place to mitigate the financial impact of events causing financial loss.	**Inspection:** Obtained and reviewed the Company's insurance policy. Verified an insurance policy was in place to mitigate the financial impact of events causing financial loss.	No exceptions noted.
9.2	The entity assesses and manages risks associated with vendors and business partners.		
9.2.1	The Company has a Vendor Management Policy, which provides guidance regarding the identification and management of critical vendors and business partners.	**Inspection:** Obtained and reviewed the Vendor Management Policy. Verified the Company had a Vendor Management Policy, which provided guidance regarding the identification and management of critical vendors and business partners.	No exceptions noted.
9.2.2	Executed agreements are maintained for key sub-service organizations. These agreements define the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	**Inspection:** Obtained and reviewed the agreements for the sub-service organizations utilized during the audit period. Verified executed agreements were maintained for key sub-service organizations. These agreements defined the scope of services, roles and responsibilities, compliance requirements, confidentiality requirements, and service levels.	No exceptions noted.

9.0 RISK MITIGATION			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
9.2.3	SOC audit reports of key sub-service organizations are reviewed for appropriateness, including complementary user entity controls.	**Inspection:** Obtained and reviewed the SOC reports and risk evaluations for the sub-service organizations utilized during the audit period. Verified SOC audit reports of key sub-service organizations were reviewed for appropriateness, including complementary user entity controls. Management required all sub-service organizations without a SOC report to fill out a questionnaire to evaluate risk.	No exceptions noted.
9.2.4	Management requires all sub-service organizations without a SOC report to fill out a questionnaire to evaluate risk.	**Inquiry and Inspection:** Inquired of management, inspected the vendor risk register, and determined there were no sub-service organizations utilized without a SOC report. Therefore, no samples were available to test. However, obtained and reviewed the Vendor Management Policy, and verified all sub-service organizations without a SOC report are required to fill out a questionnaire to evaluate risk.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
9.2.5	The Company maintains a formal Vendor Risk Management process that assesses the potential threats and vulnerabilities from vendors providing goods and services. The Company assesses, on an annual basis, the risks that critical vendors represent to the achievement of the Company's objectives.	**Inspection:** Obtained and reviewed the Vendor Management Policy. Verified the Company maintained a formal Vendor Risk Management process that assessed the potential threats and vulnerabilities from vendors providing goods and services.	No exceptions noted.

AVAILABILITY			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
A 1.1	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	Documented network monitoring policies and procedures are in place and provide guidance in the prioritization and handling of monitoring alerts and required activities that include, but are not limited to, the following: • Network communications monitoring and troubleshooting • Malicious internet activity procedures • NOC functions • Handling failure alerts • Handling site down alerts • Handling warning alerts	**Inspection:** Obtained and reviewed the Critical Systems Monitoring Policy. Verified documented network monitoring policies and procedures were in place and provided guidance in the prioritization and handling of monitoring alerts and required activities that include, but were not limited to, the following: • Network communications monitoring and troubleshooting • Malicious internet activity procedures • NOC functions • Handling failure alerts • Handling site down alerts • Handling warning alerts	No exceptions noted.
A 1.1.2	An enterprise monitoring tool is in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts are sent to security personnel.	**Inspection:** Obtained and reviewed screenshots of the system monitoring dashboard and alert configuration. Verified an enterprise monitoring tool was in place to monitor the security, performance, and availability of the network and to help identify potential sources of failure. Alerts were sent to security personnel.	No exceptions noted.
AWS is responsible for ensuring capacity demand controls are in place to meet availability commitments and requirements.			

AVAILABILITY			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
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	Documented data backup policies and procedures are in place and address the backup and recovery of production data and systems.	**Inspection:** Obtained and reviewed the backup and recovery policy. Verified documented data backup policies and procedures were in place and addressed the backup and recovery of production data and systems.	No exceptions noted.
A 1.2.2	The Company maintains recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	**Inspection:** Obtained and reviewed the Backup and Recovery Policy. Verified the Company maintained recovery strategies, such as data replication, onsite and offsite backups, and high availability strategies for critical data systems to assure the restoration of service.	No exceptions noted.
A 1.2.3	Weekly full-system and daily incremental backups are performed using an automated system.	**Inspection:** Obtained and reviewed the backup configuration. Verified weekly full-system and daily incremental backups were performed using an automated system.	No exceptions noted.
A 1.2.4	Database data is archived via replication methods on a continual basis.	**Inspection:** Obtained and reviewed the database replication configuration. Verified database data was archived via replication methods on a continual basis.	No exceptions noted.
A 1.2.5	The automated backup system notifies computer operations personnel via email of failed backup jobs.	**Inspection:** Obtained and reviewed the backup failure notification configuration. Verified the automated backup system notified computer operations personnel via email of failed backup jobs.	No exceptions noted.

AVAILABILITY			
Control #	Control Activity	Procedures Performed by the Service Auditor	Test Results
AWS is responsible for ensuring environmental protection controls are in place to meet availability commitments and requirements.			
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A 1.3.1	Management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	**Inquiry, Observation, and Inspection:** Inquired of management, witnessed the generation of a list of critical security incidents during the audit period, inspected the list, and determined there were none. Therefore, no samples were available to test. However, obtained and reviewed the Security Incident Response and Breach Policy, and verified management performs an assessment of each critical security incident, including an analysis of the completed Incident Response Plan, and signs-off on the post-mortem assessment.	Control is designed effectively; however, no samples were available to test the operating effectiveness of the control.
A 1.3.2	The Company has a comprehensive Incident Response Plan that is communicated to staff and is regularly updated. Incident response training is held annually.	**Inspection:** Obtained and reviewed the Security Incident Response and Breach Notification Manual and the most recent incident response training session detail report. Verified a comprehensive Incident Response Plan was communicated to staff and regularly updated. Additionally verified incident response training was held annually.	No exceptions noted.

AVAILABILITY			
Control #	**Control Activity**	**Procedures Performed by the Service Auditor**	**Test Results**
A 1.3.3	Incident recovery plan testing is performed annually, at minimum. The testing includes: • Development of testing scenarios based on threat likelihood and magnitude • Consideration of relevant system components from across the Company that can impair availability • Scenarios that consider the potential for the lack of availability of key personnel • Revision of continuity plans and systems based on test results.	**Inquiry and Inspection:** Inquired with Management and inspected the Business Continuity Plan and determined the plan was not tested during the audit period. Therefore, we were unable to verify The Business Continuity and Disaster Recovery Plan was tested annually using scenarios based on threat likelihood and magnitude and lack of availability of key personnel and systems.	***Exception noted. See Section 5 for further details.***
A 1.3.4	The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inquiry and Inspection:** Inquired with Management and inspected the Business Continuity Plan and determined the plan was not tested during the audit period. Therefore, we were unable to verify The Business Continuity and Disaster Recovery Plan was tested annually using scenarios based on threat likelihood and magnitude and lack of availability of key personnel and systems.	***Exception noted. See Section 5 for further details.***
AWS is responsible for managing the redundant infrastructure used and configured by Aurea for recovery operations.			

SECTION FIVE

Other Information Provided by ESW Operations, LLC

OTHER INFORMATION PROVIDED BY ESW OPERATIONS, LLC

1 Management's Response to Testing Exceptions

The information included in this section of the report is presented by ESW Operations, LLC to provide additional information to user entities and is not part of ESW Operations, LLC's description of controls placed in operation. The information in this section has not been subjected to the procedures applied in the examination of the description of controls related to the security and availability criteria and, accordingly, CyberGuard Compliance, LLP expresses no opinion on it.

Control Number	Criteria	Control Description	Test Results
6.1.11	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.	In-scope applications are configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Strong password complexity	**Inspection:** Obtained and reviewed the password configurations for the in-scope systems noting one system did not have a default password configuration and several other in-scope systems only required a minimum password length. Therefore, we were unable to verify the in-scope applications are configured to enforce the following password requirements: • Minimum Password Length • Maximum Password Age • Password History • Strong password complexity

<table>
<tr><th>Control Number</th><th>Criteria</th><th>Control Description</th><th>Test Results</th></tr>
<tr><td colspan="4">**Management’s Response:**
Customer-Specific Deployments:
For our products with customer-specific deployments, we provide flexibility by allowing customers to define and manage their own password policies within the product. This approach empowers customers to tailor their security settings according to their unique compliance and security requirements.

Strong Password Policy for Shared Products:
For products shared across multiple customers, we have implemented robust password policies designed to maintain high security standards and protect user accounts.

Remediation Plan: N/A

Target Date: N/A</td></tr>
</table>

Control Number	Criteria	Control Description	Test Results
7.3.5	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.	The Business Continuity and Disaster Recovery Plan is tested annually, at minimum, using scenarios based on threat likelihood and magnitude, and lack of availability of key personnel and systems. The plan is updated based on the test results.	**Inquiry and Inspection:** Inquired of Management and inspected the Business Continuity Plan and determined the plan was not tested during the audit period. Therefore, we were unable to verify The Business Continuity and Disaster Recovery Plan was tested annually using scenarios based on threat likelihood and magnitude and lack of availability of key personnel and systems.
7.5.1	7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
A 1.3.4	A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.		

<table>
<tr><th>Control Number</th><th>Criteria</th><th>Control Description</th><th>Test Results</th></tr>
<tr><td colspan="4">**Management’s Response:**

Cloud Infrastructure Resilience:
All our products are deployed on Amazon Web Services (AWS), which inherently provides high availability. AWS's infrastructure is designed to support seamless backups and quick recovery, mitigating many risks associated with downtime and data loss.

Regular Disaster Recovery Exercises:
While AWS offers a robust platform, we commit to conducting Disaster Recovery (DR) exercises annually to validate and ensure our readiness. These exercises are critical for testing our processes and improving them continually.

Challenges and Future Plans:
This year, we faced unforeseen internal team changes that impacted our ability to conduct the planned DR test. We consider this an exception and are taking necessary steps to prevent recurrence.

Remediation Plan:
Moving forward, we have scheduled our next DR exercise for 2025 and commit to executing these exercises annually to align with best practices and audit requirements.

Target Date: September 2025</td></tr>
</table>

Control Number	Criteria	Control Description	Test Results
A 1.3.3	A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Incident recovery plan testing is performed annually, at minimum. The testing includes: • Development of testing scenarios based on threat likelihood and magnitude; • Consideration of relevant system components from across the Company that can impair availability • Scenarios that consider the potential for the lack of availability of key personnel • Revision of continuity plans and systems based on test results.	**Inquiry and Inspection:** Inquired of Management and inspected the Business Continuity Plan and determined the plan was not tested during the audit period. Therefore, we were unable to verify The Business Continuity and Disaster Recovery Plan was tested annually using scenarios based on threat likelihood and magnitude and lack of availability of key personnel and systems.

Control Number	Criteria	Control Description	Test Results
Management’s Response: **Cloud Infrastructure Resilience:** All our products are deployed on Amazon Web Services (AWS), which inherently provides high availability. AWS's infrastructure is designed to support seamless backups and quick recovery, mitigating many risks associated with downtime and data loss. **Regular Disaster Recovery Exercises:** While AWS offers a robust platform, we commit to conducting Disaster Recovery (DR) exercises annually to validate and ensure our readiness. These exercises are critical for testing our processes and improving them continually. **Challenges and Future Plans:** This year, we faced unforeseen internal team changes that impacted our ability to conduct the planned DR test. We consider this an exception and are taking necessary steps to prevent recurrence. **Remediation Plan:** Moving forward, we have scheduled our next DR exercise for 2025 and commit to executing these exercises annually to align with best practices and audit requirements. **Target Date:** September 2025			

Control Number	Criteria	Control Description	Test Results
8.1.6	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.	Vendor security patches are evaluated, and critical patches are applied to key systems and applications within 30 days of release.	**Inspection:** Evidence of patch evaluation and application was unavailable for review. Therefore, we could not be determined whether critical patches were consistently evaluated and applied to key systems and applications within the 30-day window.

<table>
<tr><th>Control Number</th><th>Criteria</th><th>Control Description</th><th>Test Results</th></tr>
<tr><td colspan="4"><b>Management’s Response:</b>
<b>Patch Management Policy:</b>
Our internal policy is to apply patches based on the results of vulnerability scans, which are designed to identify security issues that could affect our systems. This approach ensures that we address only the vulnerabilities that are relevant and critical to our environment, thereby minimizing unnecessary modifications to the production servers.

<b>Risk-Based Approach:</b>
Most of our production servers are secured behind robust firewalls and are not exposed directly to the internet. This provides an additional layer of security, allowing us to focus our patching efforts on vulnerabilities that are real threats as identified by our scans rather than applying all available patches indiscriminately.

<b>Vulnerability Scans and Patch Application:</b>
We conduct scheduled vulnerability scans to proactively identify and evaluate potential security issues. If a vulnerability is detected, patches are prioritized and applied based on the severity of the threat and the potential impact on our systems. This ensures efficient use of resources while maintaining high security standards

<b>Remediation Plan:</b>
We are committed to continuing this practice, ensuring our systems remain secure without undergoing unnecessary changes that might arise from blanket patching. This strategy effectively balances security needs with system stability.

<b>Target Date:</b> N/A</td></tr>
</table>