# Avaamo

Report on Controls at a Service Organization Relevant to Security, Confidentiality, Availability, Privacy, and HIPAA Security Rule Requirements

## SOC 2 Type 2®

For the Period November 1, 2022 to October 31, 2023

*SOC 2 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)*

BARR ADVISORY

# Contents



*This report is intended solely for use by the management of Avaamo and its user entities (i.e., customers) that use the services covered by this report during the period. Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.*

# Section I

## Independent Service Auditor's Report Provided by BARR Advisory, P.A.

# Independent Service Auditor's Report

To the Management of Avaamo:

**Scope**

We have examined Avaamo's accompanying description of its Avaamo Conversational AI platform, titled "Avaamo's Description of Its Avaamo Conversational AI Platform," throughout the period November 1, 2022 to October 31, 2023 (description), based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Avaamo's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, availability, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*). We have also examined whether the controls stated in the description were implemented to meet the requirements set forth in 45 C.F.R. Sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act (HIPAA) (HIPAA Security Rule requirements - 2013 HIPAA Omnibus Final Rule).

The information included in Section V, "Other Information Provided by Avaamo That Is Not Covered by the Service Auditor's Report," is presented by Avaamo management to provide additional information regarding control mappings to the ISO/IEC 27001, CSA-CCM v4, NIST CSF 1.1, NIST 800-171 revision 2, and HITRUST v9.4 Frameworks has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve Avaamo's service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

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

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

Avaamo 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 Avaamo's service commitments and system requirements were achieved. Avaamo has provided the accompanying assertion titled "Assertion of Avaamo Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Avaamo 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.

Avaamo is also responsible for selecting HIPAA Security Rule requirements as additional criteria and implementing controls to meet the requirements set forth in 45 C.F.R. Sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act (HIPAA).

**Service Auditor's Responsibilities**

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

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

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

- Evaluating the overall presentation of the description.

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

**Relevant Ethical Requirements**

We are required to be independent of Avaamo and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 users may consider important to meet their informational needs.

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

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

**Description of Tests of Controls**

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV.

**Controls That Did Not Operate During The Period**

The description discusses its procedures for authorized and/or unauthorized disclosures of personal information, including notification of breaches and incidents to affected data subjects, regulators, and others. However, during the period November 1, 2022 to October 31, 2023, Avaamo did not experience any situations where any authorized and/or unauthorized disclosures, including notification of breaches and incidents of personal information, occurred that warranted the operation of such controls.

Because those controls described above did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using the following trust services criteria:

- P6.2 - The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.
- P6.3 - The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.
- P6.6 - The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

**Opinion**

In our opinion, in all material respects,

a. The description presents the Avaamo Conversational AI platform that was designed and implemented throughout the period November 1, 2022 to October 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Avaamo'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 organizations and user entities applied the complementary controls assumed in the design of Avaamo's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Avaamo's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Avaamo's controls operated effectively throughout that period.

d. The controls stated in the description were implemented and operated effectively to meet the requirements set forth on 45 C.F.R. Sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act (HIPAA).

**Restricted Use**

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Avaamo, user entities of the Avaamo Conversational AI platform during some or all of the period November 1, 2022 to October 31, 2023, business partners of Avaamo subject to risks arising from interactions with the Conversational AI platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, regulators or sponsoring organizations who developed the HIPAA Framework, all of whom 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 HIPAA Security Rule requirements; and,

- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Fairway, KS

January 31, 2024

# Section II
## Assertion of Avaamo Management

# Assertion of Avaamo Management

We have prepared the accompanying description titled "Avaamo's Description of Its Avaamo Conversational AI Platform" throughout the period November 1, 2022 to October 31, 2023 (description), based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA *Description Criteria* (description criteria). The description is intended to provide users with information about the Avaamo Conversational AI platform that may be useful when assessing the risks arising from interactions with Avaamo's system, particularly information about system controls that Avaamo 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, confidentiality, availability, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*, and the requirements of 45 C.F.R. Sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act (HIPAA) (HIPAA Security Rule requirements - 2013 HIPAA Omnibus Final Rule).

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

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

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

a. The description presents the Avaamo Conversational AI platform that was designed and implemented throughout the period November 1, 2022 to October 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Avaamo'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 organizations and user entities applied the complementary controls assumed in the design of Avaamo's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Avaamo's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Avaamo's controls operated effectively throughout that period.

d. The controls stated in the description were implemented and operated effectively to meet the requirements set forth on 45 C.F.R. Sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act (HIPAA).

**Controls That Did Not Operate During the Period**

Our description discusses its procedures for authorized and/or unauthorized disclosures of personal information, including notification of breaches and incidents to affected data subjects, regulators, and others. However, during the period November 1, 2022 to October 31, 2023, Avaamo did not experience any situations where any authorized and/or unauthorized disclosures, including notification of breaches and incidents of personal information, occurred that warranted the operation of such controls.

**Avaamo**

January 31, 2024

# Section III

## Avaamo's Description of Its Avaamo Conversational AI Platform

# Overview of Operations

**Company Background**

Avaamo is a deep-learning software company that specializes in conversational interfaces to solve specific, high-impact problems in the enterprise. Avaamo is building fundamental artificial intelligence (AI) technology across a broad area of neural networks, speech synthesis, and deep learning to make conversational computing for the enterprise a reality. The company was founded in 2014 to provide a conversational AI platform to enterprise customers across the globe.

**Description of Features Provided**

Avaamo's core application, the Avaamo Conversational AI platform (“Avaamo platform” or the “system”), is a multi-tenant, multi-user Software as a Service (SaaS) solution that helps customers create, manage, and deploy bots based on the conversational AI services. Avaamo provides a cognitive, technology driven platform that simplifies the time needed to design and deploy enterprise bots or virtual assistants (VAs) to corporate employees and their customers.

Avaamo has developed a cognitive computing platform specifically designed to support a broad range of enterprise solutions across various industries, including banking, healthcare, insurance, and telecom. Enterprise customers can create bots based on specific use cases, user journeys, and more. The following are examples of bots that have been developed on the platform:

- Banking:
    - Personal banker
    - Wealth manager
    - Relationship manager finder
- Telecom:
    - Recharge assistant
    - Customer support
    - Network operations
- Healthcare:
    - Patient guide
    - Scheduling assistant
    - Urgent care
- Retail:
    - Service advisor
    - Order tracker
    - Supplier assistant
- Insurance:
    - Underwriter assistant
    - Plan advisor
    - Policy renewal

- Service desk:
    - Employee assistant
    - Troubleshooting
    - Order management

Avaamo combines natural language understanding (NLU) and various machine learning (ML) technologies to sift through structured transaction data residing in applications, and unstructured data residing in documents, knowledge bases, or repositories to answer questions from users in real time. Like a human, the Avaamo platform learns from experience and training using Avaamo's patented approach to both assisted and supervised learning. The services, features, and technologies that support the Avaamo platform include:

- Machine Learning
- Conversational Design
- Continuous Bot Improvement
- Vertical Specialization
- Enterprise Services
- Voice

**Machine Learning:** A key part of the Avaamo platform which uses a combination of rules, statistical data, language/tone/sentiment corpus, user selection, and past user transactions to learn and predict the appropriate intent outcome to the user query. The Avaamo platform's machine learning is based on the following technologies:

- *Vertical Domains:* Avaamo comes with more than 25 pre-built vertical artificial intelligence and machine learning models to provide a head start in implementing conversations across industries, such as banking, insurance, retail, and more.
- *Advanced NLU:* Avaamo's proprietary NLU engine helps process and understand complex user queries.
- *Data Science Automation:* Sifts through data, understands the top intents, and intelligently labels and categorizes data to bootstrap machine learning models.
- *Knowledge Graph:* Provides the ability to ingest content, documents, and websites and instantly enables virtual assistants to learn and respond using that knowledge.
- *Interaction Engine*: Transcripts, services tickets, and call logs.
- *Inference Engine*: Structured tables and relational databases.
- *Document Engine*: Technical documents and marketing materials.
- *Site Engine*: Website maps and informational links.

**Conversation Design:** Provides the ability to create conversation flows directed toward a specific goal. The intent of any bot is to perform a set of tasks that direct users toward a goal. Conversation designs can include flows to troubleshoot common problems, handle billing inquiries, and more. Features include:

- *Entity Capture and Intent Classification*: Provides dynamic and adaptive conversation based on domains, languages, entities, and keywords from the end consumer.

- *Disambiguation*: Improves interactions over time based on user choices in prior interactions.
- *Contextual Content*: Automatically serves relevant content to keep users engaged during a conversation.
- *Error Correction*: Fixes spelling errors based on languages and domains.
- *Remembering Context*: Learns from past interactions and backend integrations to provide more accurate and timely responses to end consumers.
- *Frustration Handler*: Tracks emotional states of end consumers during interactions for agent escalations.
- *Feedback Collection*: Provides end consumers the ability to deliver explicit feedback to guide real-time learning and improve future interactions.
- *Non Sequiturs*: Provides personality, small talk, and conversational fluidity.
- *Flow Designer*: Enables non-technical content writers to create, design, and edit conversational flows quickly with a suite of intuitive tools.
- *Tone and Sentiment*: Detects the sentiment and tone of customers during interactions, providing the ability to build dialog strategies to adjust the conversation accordingly.
- *Dynamic Conversation Flows*: Enables dynamic generation of new multi-turn conversations from scratch using ML domains and their associated intents and entities.
- *Conversational Analytics*: Provides the ability to drill down to popular intents, channel specific usage, goal specific metrics, and other business metrics that can help drive better customer experiences.
- *Language*: Provides the ability to build bots once and instantly access them on consumer messaging apps, smart assistants, and enterprise channels (such as portals, mobile apps, etc).

**Continuous Bot Improvement:** A toolkit to help ensure continuous improvement over time. The toolkit is based on supervised deep learning technology and includes the following tools:

- *Unhandled Query Analyzer*: Helps discover new intents and reinforce old intents with new training data, based on common interactions between bots and end consumers.
- *Automatic Regression Testing*: Enables Avaamo customers to retain core functionality of bots across versions, releases, developers, etc.
- *Analytics Dashboard*: A set of visual representations of interactions to help Avaamo customers understand trends and act on new insights over time.
- *User Journey*: Provides the ability to follow individual interactions, track drop offs, and discover user personas.

**Vertical Specialization:** Provides progressively fine-tuned base models to support many industries. The models improve over time, across Avaamo's customer base, and across industries using a combination of manual fine tuning, unsupervised deep learning, and federated learning. Vertical specializations combine Avaamo's multilingual language model, base domains, industry domains, and customer-specific domains.

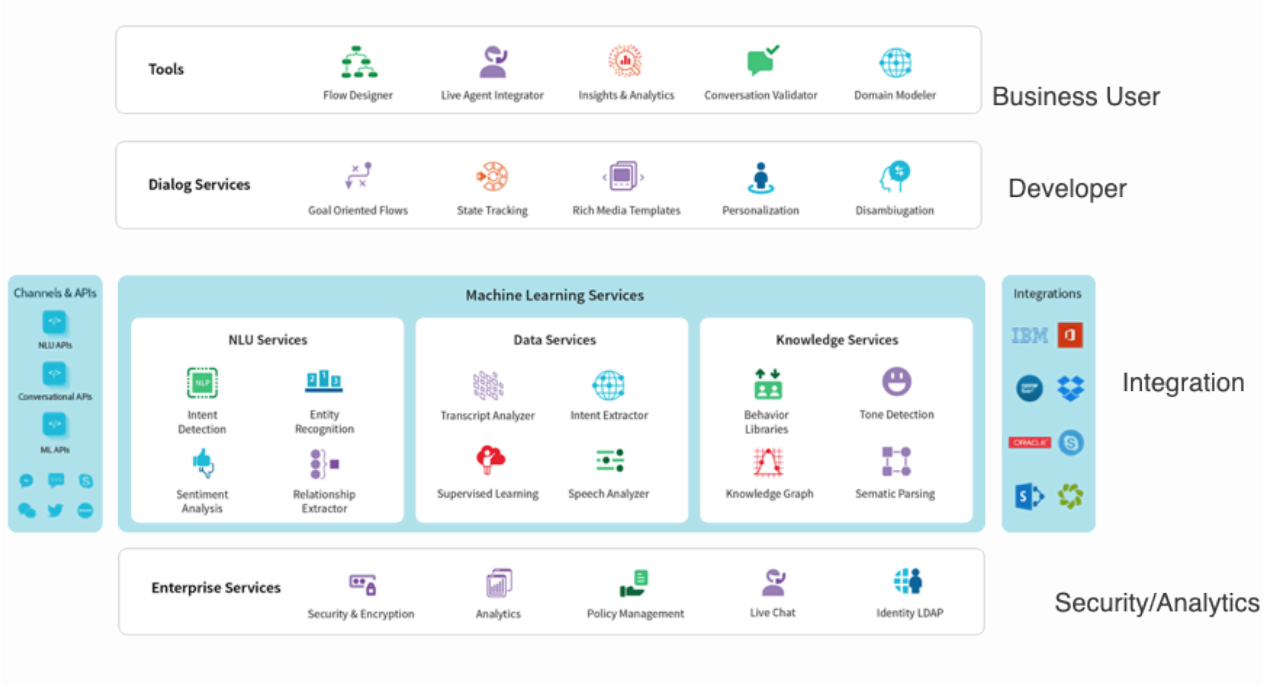
**Enterprise Services:** Avaamo provides several enterprise-ready services to help organizations get the most out of the application, including the following:

- *Integrations:* Avaamo supports integration using application programming interfaces (APIs), web services, enterprise service buses (ESBs), message queues (MQs), custom adapters, and more. Plus, it comes with 150+ pre-built integrations with business applications, such as Salesforce, Oracle, SAP, Workday, ServiceNow, and more.
- *Security and Compliance:* The Avaamo platform includes enterprise-wide security, including military grade encryption for data in transit and data at rest, access controls and entitlements, and multi-factor authentication (MFA) to protect and secure data within the application.
- *Flexible Deployment:* Avaamo includes options, based on each entity's environment, for a globally secure cloud deployment with HIPAA, PCI, FINRA compliance, a hybrid cloud deployment, or an on-premise deployment.
- *Omni-channel:* Avaamo provides the ability to build bots once and instantly access them on consumer messaging apps, smart assistants, and enterprise channels (such as portals, mobile apps, etc.).

**Voice:** Avaamo offers the SmartCall™ feature that provides an AI-powered conversational interactive voice response (IVR) for phone-based support issues. Voice includes the following components:

- *Conversational IVR:* Leverages AI and natural language processing (NLP) to provide the ability to converse naturally and provide the support required for each end consumer without having to navigate long, complicated audio menus.
- *Voice-based Assistants:* Alexa, Google Assistant, and Cortana can help workforces start dialogues with customers.

The diagram below shows a high-level architecture of the components and services described above.



There are three methods and types of users that interact with the Avaamo platform. Each method includes different abilities and services, which are summarized below:

1. *Enterprise users*: These users access the system dashboard through a web browser that provides the ability to perform the following tasks:
    - Create domain models from customer data (includes the user-agent transaction);
    - Update/manage domain models;
    - Create and manage bots;
    - Create and manage knowledge from documents, PDFs, raw data uploads, and websites, in addition to manually curated questions and answers;
    - Create and manage integrations;
    - Create and manage deployment channel configurations;
    - Analyze bot usage;
    - View and manage bot learning insights;
    - Manage dashboard users and admins; and,
    - Manage API access to the system.
2. *End consumers*: Bots are created and intended to interact with everyday consumers to assist with support cases, bill inquiries, and more. Interactions with bots occur via multiple channels including, but not limited to, the following:
    - Web widgets;
    - Skype;
    - Phone;
    - Meta Messenger;
    - Workplace from Meta;
    - WhatsApp;
    - Mobile phones;
    - Amazon Alexa; and,
    - SMS.
3. *Avaamo internal users*: A unique admin dashboard used to create customer accounts, perform analysis on bot usage across all Avaamo customer accounts, and improve the application for future releases. Once a customer account is created, Avaamo's internal employees no longer have access to customer instances unless explicitly requested, authorized, and provisioned by customer admin users.

**Principal Service Commitments and System Requirements**

Avaamo designs its processes and procedures related to the Avaamo platform to meet its objectives. Those objectives are based on the service commitments that Avaamo makes to user entities, the laws and regulations that govern the provision of Avaamo platform services, and the financial, operational, and compliance requirements that Avaamo has established for the services.

Avaamo is subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdiction in which Avaamo operates.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments are standardized and include, but are not limited to, the following:

- Technical configurations to ensure users access the information they need based on their role in the system through the principle of least privilege;
- The use of identity access management software and controls for usernames, passwords, access provisioning and de-provisioning, and role-based access;
- Procedures for managing security incidents and breaches, including notification procedures;
- Regular vulnerability scanning and penetration tests over the Avaamo platform and supporting infrastructure components; and,
- Use of boundary protection systems, including web application firewalls (WAFs) and firewalls.

Confidentiality commitments are standardized and include, but are not limited to, the following:

- Confidential information must be used only for the purposes explicitly stated in agreements between Avaamo and the customer;
- Use of encryption technologies to protect customer data both at rest and in transit; and,
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.

Availability commitments are standardized and include, but are not limited to, the following:

- Regular maintenance to be performed outside regular business hours and notice of any emergency maintenance performed outside of documented maintenance windows;
- Real-time information and updates on the status of the Avaamo platform, including uptime reporting via status.avaamo.com; and,
- Responses to customer-reported issues within 24 business hours.

Privacy commitments include, but are not limited to, the following:

- Communication to system users regarding the notice, choice and consent, collection, use, retention, disclosure, and disposal of personal information;
- Personal information is collected consistent with the organization's privacy commitments and system requirements;
- Notification of security breaches within 30 days; and,

- Data subject request (DSR) process to provide data subjects with information upon request when identified and authenticated.

HIPAA commitments include, but are not limited to, the following:

- Electronic protected health information (ePHI) in transit is protected and safeguarded with only those who have a business need to see and access this information; and,
- Business associate agreements (BAAs) are in place with any downstream business associates who transmit ePHI on behalf of Avaamo.

Service requirements are communicated in Avaamo's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Avaamo platform.

**Components of the System Used to Provide the Services**

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

**Infrastructure and Software**

The Avaamo platform is a Linux client-server application developed and maintained by Avaamo's in-house software engineering team. The software engineering team enhances and maintains the software to provide conversational AI service for the company's customers in multiple verticals. The internal computing platforms and global infrastructure supporting the Avaamo platform are provided by Amazon Web Services (AWS).

The system is only accessible over Secure Sockets Layer (SSL). Avaamo internal users are authenticated via a unique user ID and password combination. Avaamo customers access publicly facing servers using HTTPS. Besides the functional aspect of the site, role-based security is used for Avaamo site administration. All customer data is encrypted at rest and in transit, and traffic between all external web application integration is done over HTTPS. Avaamo also undergoes annual penetration tests from a third-party security firm. To further minimize Avaamo’s attack surfaces, public-facing services are limited to the AWS load balancers and AWS WAF is deployed to monitor traffic with the web application.

The software engineering team ensures system code is algorithmically efficient, reducing the number of layers, and using caching where applicable. Databases utilize a data model designed with appropriate indexes to facilitate access patterns.

Avaamo is responsible for managing the development and operation of the Avaamo platform, including development, maintenance, and infrastructure components such as servers, databases, and storage systems. The in-scope Avaamo infrastructure and software components are shown in the table below:

| Primary Infrastructure and Software | | | |
|---|---|---|---|
| **System/ Application** | **Business Function/Description** | **OS DB** | **Physical Location** |
| Avaamo Conversational AI Platform | Conversational AI bot platform designed to enable enterprises to rapidly develop and deploy bots for use by employees and customers. | Ubuntu Linux/MySQL RDS | AWS Multiple Availability Zone (MAZ) |
| Avaamo Admin Dashboard | Admin portal used by internal Avaamo administrators to provision and deprovision customer accounts. | Ubuntu Linux/MySQL | AWS Multiple Availability Zone (MAZ) |
| AWS Identity and Access Management (IAM) Console | Provides the underlying infrastructure components to create the environments in which the Avaamo system is hosted from. | AWS Proprietary | AWS Cloud |
| AWS WAF | A web application firewall that helps protect Avaamo's web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. | AWS Proprietary | AWS Cloud |
| AWS Relational Database System (RDS) | Provides services to allow for scalable MySQL deployments in the cloud for database management. | AWS Proprietary | AWS Multiple Availability Zone (MAZ) |
| GitLab | Source code repository and version control system. | GitLab Proprietary | GitLab Cloud |
| OpenVPN | Cloud-based virtual private network (VPN) tool used by Avaamo engineers to authenticate as administrators to Linux resources within the AWS environment. | OpenVPN Proprietary | OpenVPN Cloud |
| AWS Elastic Compute Cloud (EC2) | AWS web service that provides resizable compute capacity in the cloud through the use of EC2 instances and load balancers. | AWS Proprietary | AWS Cloud |
| Amazon Simple Storage Services (S3) | Provides an interface to store and retrieve information, such as avatars for bots and files shared within bots. S3 provides bucket- and object-level access and version control, and is managed through the AWS IAM interface. | AWS Proprietary | AWS Multiple Availability Zone (MAZ) |

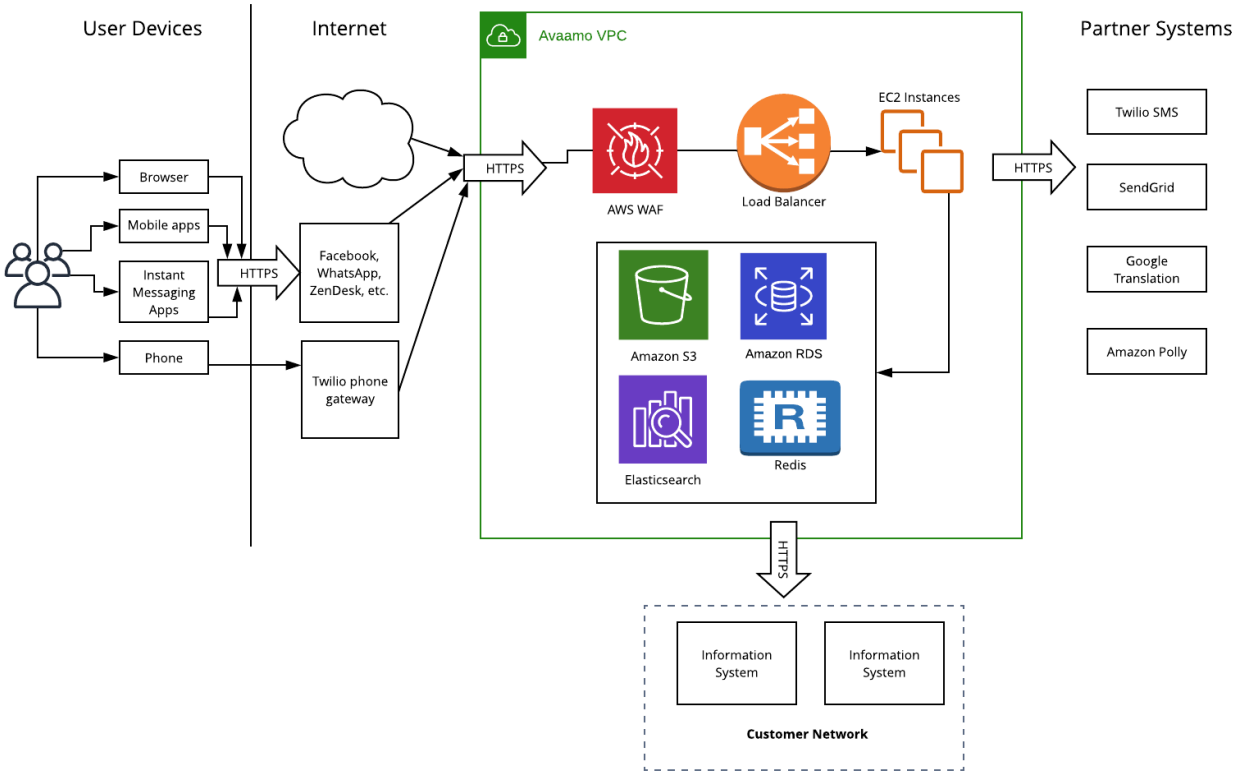
 

| Supporting Infrastructure and Software | |
|---|---|
| **System/Application** | **Business Function/Description** |
| SendGrid | Tool used to send emails from the Avaamo platform. |
| YouTrack | A customizable tool for agile software development that Avaamo uses to log and track progress for bugs, tasks, features, and projects. |
| Bugsnag | A tool used to track errors within the Avaamo platform. |
| Twilio | A telephony infrastructure web service that allows Avaamo to use standard web languages to integrate phone calls, text messages, and IP voice communications into their web, mobile, and traditional phone applications. |
| Graylog | Centralized log management solution built to open standards for capturing, storing, and enabling real-time analysis of application activity. |
| Prometheus | Open-source monitoring tool used to monitor for key availability metrics such as CPU, process failures, and disk space. |
| Fluentd | Open-source data collector used for unified logging. |
| Google Translation | A Google Cloud service that provides the ability to dynamically translate between languages using Google machine learning. |
| Google Workspace | Internal file sharing, company email, and document storage. |
| Statuspage.io | Real-time information and updates on Avaamo platform services. |
| Zoom.us | Video conferencing software used by Avaamo teams to communicate with customers and Avaamo team members. |
| PagerDuty | Alerting tool that integrates with Avaamo's various monitoring tools to provide real-time alerts and escalations when issues arise. |
| Rippling | Mobile device management software used to manage Avaamo laptops. |
| KnowBe4 | Learning management system used to deliver Avaamo's security awareness training program to employees. |
| Amazon Polly | Text to speech service. |
| Elasticsearch | A distributed RESTful search and analytics engine that supports backend functions of the Avaamo platform. |
| AWS Systems Manager | Provides an interface for the secure distribution and installation of software packages. |
| Azure OpenAI | Large language models (LLMs) to power conversational AI capabilities. |
| Redis | In-memory data structure that provides a distributed, in-memory key value database within the Avaamo platform. |

| Supporting Infrastructure and Software | |
|---|---|
| **System/Application** | **Business Function/Description** |
| Zendesk | Ticketing system used for customer support and sales. |
| Ansible | Open-source code management tool for software provisioning, configuration, and application deployment. |
| AWS CloudWatch | Operational metrics monitoring over the AWS environment. |
| Brakeman | Static analysis security vulnerability scanner. |

**Overall Technical Diagram**




## People

Avaamo has a staff organized in the following functional areas:

- *Corporate*: Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources. Corporate is responsible for oversight of the development and performance of internal control.
- *Operations*: Manages the configuration and monitoring of the Avaamo platform.
- *Engineering:* Develops and supports the development life cycle management activities, including software design, coding, quality assurance, security testing, deployments, and documentation.
- *Finance and Administration:* Oversees the operations, human resources, and accounting operations.
- *Marketing:* Designs customer and partner communication, social media, and all content to support Avaamo operations.
- *Sales:* Product and domain experts who focus on demoing and selling the Avaamo platform.

- *Information Security*: Responsible for the management of information security throughout the organization. Assesses security risks on an ongoing basis through regular management meetings with IT personnel, reviewing and acting upon security event logs/incidents, performing vulnerability assessments, and conducting a formal annual risk assessment in conjunction with company wide risk assessments.
- *Security Governance Team (SGT)*: Maintains security credentials and is responsible for developing, maintaining, and enforcing Avaamo's information security policies and program including the performance of internal audits. Also responsible for the independent oversight of the development and performance of internal control.
- *HIPAA Security Officer:* Responsible for oversight of the HIPAA compliance program, HIPAA policies and procedures, and activities/projects involving ePHI.

**Data**

Data processed, stored, and transmitted by the Avaamo platform is managed by both Avaamo and customer enterprises. The bot developers access the dashboard via a browser using their one-time use passcode. They develop the bots as per their business use-cases, and simulate the user interactions. Almost all real bots involve some integration with customers' backend systems like enterprise resource planning (ERP), customer relationship management (CRM), databases and file systems, and more. Avaamo recommends multiple ways to secure the integrations.

All data users exchange with the bot and the bot responses shown to the users, including the responses generated from the backend systems, are stored within the Avaamo platform.

Data processed, stored, and transmitted by the Avaamo platform includes, but is not limited to, the following:

- Admin logins
- Bot runtime data, which includes messages the bot exchanged with users
- Bot insights
- Bot analytics data
- System files
- Error logs
- User Information

**Data Classification**

Data within the Avaamo platform comes from various sources, including manual input from customer users, messaging applications, connections with customer systems, and bot interactions. Each customer's data is segmented from other customers' data.

Avaamo has a Data Classification and Handling Policy in place that defines system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policy is reviewed and approved on at least an annual basis by members of the SGT.

Information assets, including customer data, are assigned a classification level based on the audience for the information. The classification level then guides the selection of protective measures to secure the information.

The table below provides examples of the data processed, stored, and transmitted by the Avaamo platform, and the classification label applied to each example.

| Classification | Description | Examples of Data |
|---|---|---|
| Customer Confidential | Avaamo shall monitor client data classification levels in accordance with client contractual terms or commitments. The client data in this case is every interaction users have with the bot and the bot responses, including responses generated from backend system data. For example, when user requests "What is the status of my ticket #123456?" the bot would respond with "Your ticket #123456 is complete. Please contact your manager 'Mr. Manager' for additional information." | • Messages between bots and users<br>• User accounts<br>• Email addresses<br>• First and last names<br>• Permissions<br>• ePHI |
| Confidential | Unauthorized disclosure and compromise or destruction of this type of information would, directly or indirectly, have an adverse impact on Avaamo, its customers, or employees. This data may only be shared with those who have a relationship with Avaamo, if they have signed a non-disclosure agreement, and have a "need to know." This could include information regarding customers, personnel, payroll, etc. | • Error logs<br>• Bot success rates and details, such as successful queries, disambiguations, unhandled issues, and agent transfers<br>• Bot analytics, such as total queries, top queries, user feedback, and top intents<br>• Bot definition metadata including domains and knowledge<br>• Employee files (payroll details, tax forms, etc.) |
| Private | If disclosed, this information would provide access to business secrets and could jeopardize important interests or actions of Avaamo or its customers. Characterized as sensitive information that is intended for a very limited group of individuals who should be specified by name rather than their role, disclosure of this information to unauthorized persons would result in serious personal or financial exposure. This could include strategic planning information prior to general or public disclosure, passwords, or any form of security key, etc. | • System files |

| Classification | Description | Examples of Data |
|---|---|---|
| Public | Can be disclosed to anyone. Would not violate an individual's rights to privacy. Knowledge of this information does not expose Avaamo to financial loss, embarrassment, or jeopardize the security of Avaamo assets. | • Real-time information and updates on Avaamo platform services<br>• Marketing brochures<br>• Published annual reports<br>• Press releases |

**Processes and Procedures**

The security governance team has developed formal IT policies and procedures that describe incident response, network security, encryption, and system security standards. Information security policies, including sanctions for policy violations, are approved by the chief information security officer (CISO), security operations team, compliance manager, and operations team at least annually and published on the company's shared drive and can be accessed by any Avaamo team member. All teams are expected to adhere to Avaamo policies and procedures that define how services should be delivered.

The policies and procedures used to safeguard Avaamo systems and data include:

- Security Management and Governance
- Acceptable Use
- Access Control
- Awareness and Training
- Personnel Security
- Physical and Environmental Security
- Data Classification and Handling
- Incident Management
- Threat and Vulnerability Management
- Asset Management
- Change Management
- Endpoint Protection
- Risk Management
- Third Party Risk Management
- Business Continuity and Disaster Recovery

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

The applicable trust services criteria and HIPAA Security Rule requirements were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria, HIPAA Security Rule requirements, and related controls are included in Section IV, they are an integral part of Avaamo's description of the Avaamo platform. This section provides information about the five interrelated components of internal control at Avaamo, including:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities

## *Control Environment*

**Management's Philosophy and Operating Style**

Senior management has frequent interactions in both formal and informal settings, such as regularly scheduled management meetings. Meetings to address general management issues are held on a regular basis to facilitate communication and the decision-making process. Management places importance on controls and security in its processes, policies, procedures, and organizational structure. In designing its controls, Avaamo has taken into consideration the relevance of controls to meet its security, confidentiality, availability, and privacy commitments, and achieve the objectives established by the information security management system (ISMS).

A security management plan includes an information security function with defined security roles and responsibilities approved by the security committee or CISO equivalent role. The SGT maintains security credentials and is responsible for developing, maintaining, and enforcing Avaamo's information security policies and program including the performance of internal audits. The SGT is responsible for the oversight of internal control and includes members independent from control operators.

Avaamo has an organizational chart that includes defined structures and reporting lines with assigned authority and responsibilities to meet business requirements.

**Human Resources Policies and Practices**

Human resources (HR) policies and practices are documented and maintained by HR. These policies are available to Avaamo employees within the shared policy repository. HR controls exist to help ensure that qualified and competent people are recruited, developed, and retained to achieve Avaamo goals. These include controls for hiring, training, evaluating, promoting, and compensating associates.

Candidates are evaluated against the job requirements documented in job descriptions through a formal interview process. Candidates for positions involved in the development, maintenance, and security of the Avaamo platform also undergo competency evaluations, such as coding tests. Avaamo's standard employment offer letter contains a provision making the offer contingent on successful background and reference verification checks. Background or verification checks are performed on Avaamo personnel within 10 business days of hire date, as permitted by local laws.

New employees are provided with an employee handbook that must be reviewed and acknowledged by each new hire during the onboarding process. The handbook includes a statement of confidentiality, Code of Conduct, and conflict of interest agreements.

Avaamo performs formal evaluations at least annually of resourcing and staffing, including assessment of employee qualification alignment with entity objectives.

If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

## *Risk Assessment*

Avaamo reviews the risks that may threaten the achievement of its service commitments and system requirements related to the applicable trust services criteria set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, and Confidentiality* (AICPA, Trust Services Criteria) and the HIPAA Security Rule requirements of 45 C.F.R. Sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act (HIPAA) (HIPAA Security Rule requirements - 2013 HIPAA Omnibus Final Rule).

The information security function assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual risk assessment in conjunction with company wide risk assessments.

The annual risk assessment is communicated by the information security function and approved by senior management. As part of the assessment, risks affecting the organization and recommended courses of action are identified and discussed. Where applicable, mitigating controls are recommended and implemented to address the risks.

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, management considers fraud factors in each risk evaluated during the risk assessment process.

### Vendor Management

Avaamo evaluates key vendors (i.e., subservice organizations), including cloud service providers, upon agreement of service and conducts a refresher at least annually. The evaluations include a review of applicable software or other agreements, attestation reports (e.g., SOC 2, ISO 27001), and security white papers. If necessary, mitigating controls are implemented by Avaamo to address any gaps in the vendors' controls.

Senior management, as part of its annual Information Security Policy review, considers developments in technology and the impact of applicable laws and regulations on Avaamo's security policies. Security risks related to external parties (such as contractors and vendors) are identified and addressed based on its procurement and third party risk management program. Third party risk assessments are performed annually as part of the third party risk management program to ensure that attestation reports and business associate agreements are evaluated when applicable. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements.

Changes in security threats and risks are reviewed by Avaamo and updates to existing control activities and information security policies are performed as necessary.

## *Control Activities*

### Physical Security and Environmental Controls

No servers or computer facilities for the Avaamo Conversational AI platform are hosted on site. All computer facilities and access thereto are controlled at AWS data centers and OpenVPN. Avaamo reviews attestation (e.g., SOC 2) reports from AWS on an annual basis to ensure appropriate physical and environmental security controls are in place and operating effectively. Therefore, controls related to physical security are the responsibility of the subservice organizations and are described in the complementary subservice organization controls presented in this system description.

### Security Management and Awareness

Avaamo has a dedicated information security team consisting of a security officer and senior security specialist responsible for the management of information security throughout the organization. They hold positions on the SGT, maintain security credentials, and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Avaamo's information security policies. The ISMS policies are reviewed annually by the CISO, security operations team, compliance manager, and operations team. The policy is also reviewed and approved by the SGT.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

Avaamo maintains training programs to promote awareness of information security and HIPAA requirements as defined in the Security Awareness Policy. Trainings are conducted for all employees within 30 days of hire and each year thereafter.

During new hire and annual security and HIPAA training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

**Asset Management (Hardware and Software)**

Avaamo maintains an IT asset inventory that includes a list of all hardware and software components, desktops, laptops, mobile devices, as well as related descriptions for their functionality and various uses. The inventory includes information such as:

- Make and model
- Location (address of site or facility where the asset is located)
- Serial number or other method of unique identification
- Patch level
- Asset owner
- Data classification

Procedures are also in place to handle lost or stolen devices. All IT assets assigned to Avaamo are returned upon termination of employment.

**Logical Security**

*Identification and Authentication*

Avaamo's systems are safeguarded through user identification and authentication, ensuring only authorized users are able to perform actions or access information on a workstation or network as required by job function. Access to Avaamo systems requires a unique user ID and password and/or key assigned to each employee.

Avaamo's identification and authentication policies define minimum password requirements. Minimum password requirements, where technically feasible, are as follows:

- Eight-character minimum
- Multi-factor authentication or configured to expire
- Accounts are locked after six failed logon attempts
- Accounts are automatically logged out after a defined period of inactivity

Administrator access to AWS management console requires MFA, where a user must enter their AWS user ID and password, plus a verification code sent to the user's mobile device. Access keys within the AWS environment are rotated every 90 days.

Powerful access to the Linux operating system is achieved through the use of a bastion host and VPN. The bastion host is configured to only allow connections from the IP address assigned to the VPN tool. To gain access to the Linux OS, the user must have a unique VPN key installed on their device and Secure Shell (SSH) public/private keypair.

*Access Control and Management*

New user access requests are approved by the employee's manager through formal access requests. Once approved, system administrators are responsible for provisioning access based on the request and the employee's job responsibilities based on least privilege access principles.

The ability to create or modify users and user access privileges is limited to authorized personnel. Users are assigned a user role to restrict access to information resources based on the individual's role and responsibilities within the organization.

Terminated user access is removed and/or disabled within 12 hours upon the individual's change of role or responsibilities within the organization or departure from the organization. To assist in the validation of users' access and/or the removal of terminated associates, an annual access review is performed by system administrators and management. The review includes procedures to identify accounts and/or roles and permissions no longer necessary for the user to perform their job responsibilities. The access review is formally documented and includes evidence that any issues identified in the review are resolved.

Privileged accounts, roles, and permissions are assigned only to employees whose job responsibilities require access. This includes limitations on the users who have the ability to manage infrastructure systems, deploy changes, add, modify, or delete customer accounts, and access environments where customer data may reside.

**Systems and Communications Protections**

*Firewalls and Security Groups*

AWS WAF is used to protect the Avaamo Conversational AI web application from common web exploits that could affect application availability, compromise security, consume excessive resources, or result in unauthorized disclosure of data. Avaamo configures the AWS WAF service to control traffic to all web-facing instances of the Avaamo platform. Avaamo's AWS WAF is configured to prevent attacks, such as SQL injection and cross-site scripting attacks. If the WAF identifies any malicious requests, it automatically filters that request out and allows all remaining requests through the load balancers.

AWS security groups are used to manage all traffic to and from the Avaamo platform components. Inbound and outbound traffic is restricted to that which is necessary for the target environment, and specifically denies all other traffic. All unnecessary ports, protocols, and services are disabled. External traffic with the web application is routed through load balancers configured to only accept traffic over HTTPS. Remote access to the Linux OS is restricted to a bastion host that only accepts connections from the VPN tool. The database instances only allow traffic from internal IP addresses, ports, and protocols.

*Data Security*

Avaamo encrypts sensitive information at rest, in transit, and in use. Production RDS and S3 storage instances are encrypted at rest using AWS features. Sensitive information is encrypted in transit and in use using a combination of Transport Layer Security (TLS), Internet Protocol Security (IPsec), and SSH over public networks.

The Avaamo platform also provides customers with the ability to request to delete any content within the application. Requests are received by customer support and, once the data deletion activities are completed, the software is rendered unreadable systematically.

**Vulnerability Management**

*Penetration Testing*

External penetration tests are performed at least annually and include a full scope of blended attacks, such as wireless, client-based, and web application attacks. Annual exercises are performed to test organizational readiness to identify and stop attacks or to respond quickly and effectively. Identified vulnerabilities are routed through incident and risk management processes for resolution.

*Patch Management*

Avaamo has established patch baselines, which are deployed, monitored, and managed using AWS Systems Manager. Patches are applied according to the severity and impact on the infrastructure systems supporting the Avaamo platform. Security or critical patches to operating systems are applied immediately. All others are reviewed and applied based on severity, applicability, and impact on Avaamo system components.

*Baseline Configuration Hardening*

Avaamo maintains documented security configuration standards, including secure images or templates, for all authorized operating systems and software in the enterprise. Any new system deployment, or existing system that becomes compromised, is imaged using one of these master images or templates.

The Linux operating systems are hardened against the applicable Center for Information Security (CIS) benchmarks. Avaamo monitors the CIS website for changes to the hardening best practices and applies them to image templates as needed.

**Mobile Device Management**

Rippling is used to manage all laptops assigned to Avaamo. All laptops are provisioned with Rippling upon assignment to an employee and cannot be disabled by the end user. Rippling enforces protections, such as full-disk encryption, the ability to remotely wipe/lock the device, remote management of macOS restrictions, and 'Lost Mode,' which displays a customized lock screen on the device and shows its location.

**Change Management**

Changes to the Avaamo platform follow formal change control procedures to ensure that they are tested (when applicable) and only authorized changes are implemented into the production environment. Change control procedures include:

- Identification and recording of significant changes;
- Planning and testing of changes;
- Assessment of the potential impacts, including security impacts, of such changes;
- Formal approval procedure for proposed changes from application, system, or business owners;
- Communication of change details to relevant persons;
- Back-out procedures; and,
- Audit trail of changes.

Changes are documented within the YouTrack ticketing system with requirements for specific mandatory fields to be completed to perform appropriate risk evaluation and to enable effective coordination and communication within the change process.

Development and testing efforts are performed in development and QA environments that are logically separated from the production environment. These non-production environments are scrubbed of any customer or personal information using scripts to ensure sensitive information isn't used in developing or testing efforts. The QA and development environments are also designed in such a way to replicate the production environment to provide an accurate testing environment.

Developers utilize a version control application to manage application development and maintenance activities. The version control software tracks and records changes made to code repositories maintained within the software, and tracks modifications made to source code, which include the following: revision number, date/time of the revision, user responsible for the change, and any additional comments made by the developer. Developers utilize the comment field to communicate the associated change request number in the ticketing system and to include a brief description of the application code modification that was made.

Access to the version control software is restricted to user accounts accessible by authorized personnel.

QA personnel are responsible for testing and approving changes prior to implementation. Evidence of the approval is documented and tracked within the YouTrack ticketing system. After QA approves (verifies) that the change is ready for implementation, development personnel notify the engineering team that the change is ready for implementation into production. The responsibility for application change implementation resides with the engineering team.

Avaamo notifies customers of any major release and makes release notes available outlining key changes to the system on Avaamo's public-facing support site (docs.avaamo.com).

*Software Security Assurance*

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Static analysis tools are used to verify that secure coding practices are being adhered to for internally developed software. Issues identified follow a process to accept and address reports of software vulnerabilities.

**Incident Monitoring and Response**

Documented incident response policies and procedures are in place to guide personnel in incident response and server and network outage response, escalation, and resolution activities. These policies and procedures are communicated to internal users, via the incident response plan, which is available on the internal collaboration tool. For external users, Avaamo communicates the incident reporting and response procedures via customer agreements, their website, and ongoing communications. Incidents affecting systems and network devices, including issues related to availability of services and performance-related issues, are logged in ticketing systems by information security or operations personnel. The ticketing systems provide the means to document, track, notify, and escalate system incidents that are reported via the enterprise monitoring application or manually generated by a member of the information security or operations team. Incidents are classified based on the severity and include an initial description of the incident and can be linked to an impacted asset (e.g., server).

System components are continuously monitored by the Avaamo platform information security and operations teams to help ensure secure operation and availability of the system. Internal monitoring systems operate on a 24 hour per day basis to assess system availability and performance. Network and system activities that are monitored include, but are not limited to, the following:

- Availability;
- Utilization of resources, including CPU and memory usage;
- Security control mechanisms (e.g., firewalls, level 3 routers, etc.);
- Processing capacity;
- Overloads; and,
- Inbound/outbound communications for unusual or unauthorized activities including the presence of malware (e.g., network intrusions, malicious code, spyware, adware, etc.).

Avaamo's information security and operations teams utilize a variety of applications to monitor the availability and performance of Avaamo services. The monitoring applications generate on-screen and email alerts in the event that predefined thresholds are exceeded on monitored systems. Operational incidents are documented and responded to according to defined event and (if necessary) incident response processes.

Avaamo also has defined procedures for receiving, triaging, tracking, and resolving incidents reported by external parties, including customers and contractors. Issues are assigned to support personnel, categorized according to the severity of the issue, and resolved according to the same severity. Resolutions are communicated back to the reporting user according to the SLAs and official agreements.

**Availability**

Avaamo has a business continuity and disaster recovery (BC/DR) plan that is reviewed, updated, and tested at least annually. The DR plan includes recovery time and recovery point objectives for key systems and data. Runbooks, policies, procedures, and the overall BC/DR plan are updated based on the lessons learned from each test.

Avaamo utilizes automated backup systems to perform regularly scheduled backups of production systems and data. This helps to ensure that backup data is readily available, should a system failure occur. These automated backup systems are configured to perform logical full backups of production data with daily incremental backups. All data and systems are hosted at high availability data centers that provide greater than 99.99% SLA commitments for uptime.

Data and systems in AWS are also available across multiple availability zones. AWS provides services that support multi-AZ automatically, such as RDS with native cross-region replication and ElastiCache. AWS Elastic Load Balancers are used where routing is needed to manage access to the multi-AZ assets.

In addition, processing capacity is monitored through automated tools that alert operations. Issues, if any, are resolved through incident management processes.

**Confidentiality**

Avaamo has confidentiality commitments with their customers as described within terms and conditions set forth within master service agreements, which must be signed before services start.

Also, business associate agreements are in place with business associates who store ePHI. In addition, Avaamo establishes agreements, including non-disclosure agreements and HIPAA BAAs, for preserving confidentiality and privacy of information and software exchanges with external parties.

In addition, Avaamo has documented policy and procedure documents to support customer commitments which include the Information Security Policy and Data Classification and Handling Policy. Collectively, these policies provide Avaamo employees with appropriate insight into the required procedures to help ensure customer data remains confidential.

Customer data is disposed of in accordance with the requirements defined within the Data Classification Policy where processes for the disposal of data and ePHI are defined.

**Privacy**

Avaamo has a Privacy Policy published on its website where it communicates its procedures in regards to the notice, choice and consent, collection, use, retention, disclosure, and disposal of personal information, and is reviewed by management on an annual basis, and includes the following elements:

- Notice
- Choice and consent
- Collection
- Use, retention, and disposal
- Disclosure to third parties
- Security for privacy
- Quality
- Monitoring and enforcement

Updates to the policy are communicated to users of the system when material changes are made.

Additionally, Privacy Policy documents support customer privacy commitments which include a Personal Data Collection Policy, Cookie Policy, data subject rights for individuals in the European Economic Area (EEA), data security, Data Retention Policy, and notification of data breach.

Avaamo informs customers of its security and privacy commitments within master service agreements (MSAs), terms of use, and Privacy Policy, and makes the terms of use and Privacy Policy available to customers to review at any time on the Avaamo website. MSAs must be signed before services start. The privacy commitments which include consenting to the collection, use, retention, disclosure, and disposal of personal information are acknowledged to by the users of the system via the signing of the MSAs.

Personal information is collected consistent with the organization's privacy commitments and system requirements. Avaamo retains personal information consistent with its privacy commitments and as long as it is required for its intended purpose. Information is disposed of in a secure manner in accordance with policy.

Avaamo has a data subject request process to provide data subjects with information upon request when identified and authenticated. If the organization is unable to identify and authenticate, rationale for the access denial is provided.

Avaamo maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws. In addition, they have policies and procedures regarding the handling of authorized and/or unauthorized disclosures of information having to deal with privacy commitments. Avaamo records instances of authorized and unauthorized disclosures to meet the entity's objectives related to privacy. Avaamo provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

Avaamo does not maintain direct relationships with data subjects. As such, this is the responsibility of Avaamo's user entities and, therefore, controls related to P5.1, P5.2, and P6.7 are the responsibility of the user entities and are described in the complementary user entity controls presented in this system description.

## *Information and Communication*

Avaamo maintains internal informational websites, instant messaging channels, and collaboration sites describing the system environment, its boundaries, user responsibilities, and services. System documentation, including guides for configuring systems and handling customer-reported incidents, are published on internal collaboration sites. Staff are also provided access to the information security policies and procedures that support Avaamo's ISMS and commitments to customers.

Standard service agreement between customers defines service levels, when applicable, and rules of use, and additional terms for governing each service product. In addition, procedures are in place to ensure Avaamo customers and partners are informed of important events, such as major releases, incidents, and maintenance that could impact them. Release notes are published prior to any production release on Avaamo's public-facing support site (docs.avaamo.com). Customer-reported incidents are received through Avaamo's ticketing system and tracked to resolution. End users are notified any time a ticket is updated and resolutions are communicated from Avaamo support personnel.

## *Monitoring Controls*

Avaamo's monitoring controls, in addition to the incident monitoring control activities above, include procedures to evaluate the effectiveness of its security program, controls, policies, and procedures.

Performance monitoring is done using the Prometheus monitoring tool and Statuspage.io, with PagerDuty as the alerting mechanism. Alerts are triaged and routed through appropriate incident management processes for tracking to resolution.

Periodic reviews are performed over logical access, audit logs, vendor compliance, and employee performance. The risk assessment process also includes an evaluation of the existing controls to identify potential gaps in those controls, validate ownership of key controls and processes, and plans to implement new controls or modify existing controls. The security governance team is responsible for monitoring the effectiveness of the control activities and overall security program at Avaamo.

Information security key performance indicators (KPIs) are monitored and reviewed monthly for compliance status. Examples of KPIs monitored by Avaamo include vulnerabilities identified, enforcing SSL, patch level, security compliance, and critical vendor risk. Metrics that fall outside of predefined thresholds have a documented remediation plan. KPIs that fall outside of the thresholds are remediated and followed up on during monthly KPI report reviews.

Independent internal control evaluations are performed at least annually against the ISMS objectives, service commitments, and compliance objectives. Reviews are performed by the governance team and any non-conformities identified are tracked and remediated in a ticket.

**Changes to the System During the Period**

There were no changes that are likely to affect report users' understanding of how the Avaamo Conversational AI platform is used to provide the service during the period from November 1, 2022 to October 31, 2023.

**Disclosure of Incidents**

There were no system incidents during the period from November 1, 2022 to October 31, 2023, requiring disclosure that either:

- Were the result of controls failing; or,
- Resulted in a significant impairment to the achievement of systems requirements or service commitments to customers.

# Complementary User Entity Controls

Avaamo controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria and applicable HIPAA Security Rule requirements identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Avaamo customers, related to the information processed.

For customers to rely on the information processed through the Avaamo platform, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the Avaamo Conversational AI platform periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the Avaamo Conversational AI platform.
- User entity is responsible for removing terminated employee access to the Avaamo Conversational AI platform.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Avaamo Conversational AI platform according to the contract and/or statement of work.
- User entity is responsible for sending data to Avaamo via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying Avaamo if they detect or suspect a security incident related to the Avaamo Conversational AI platform.
- User entity is responsible for reviewing email and other forms of communications from Avaamo, related to changes that may affect the Avaamo customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the Avaamo website or their deployment of the Avaamo Conversational AI platform.
- User entity is responsible for communicating to Avaamo specific confidentiality and privacy configurations and commitments, including data retention, disposal, and privacy handling within the system.
- User entity is responsible for performing periodic vulnerability scanning over their deployment of the Avaamo Conversational AI platform and communicating issues to Avaamo for resolution.

- User entity is responsible for granting identified and authenticated data subjects the ability to access their stored personal information or review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy.
- User entity is responsible for correcting, amending, or appending personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy
- When access to stored personal information or request for correction is denied, the user entity is responsible for informing of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
- The user entity is responsible for providing data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.
- User entity is responsible for establishing agreements, including non-disclosure agreements and HIPAA BAAs, for preserving confidentiality and privacy of information and software exchanges with Avaamo.

# Complementary Subservice Organization Controls

Avaamo uses subservice organizations for data center hosting and infrastructure services in support of its Avaamo Conversational AI platform. Avaamo's controls related to the Avaamo Conversational AI platform cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria and HIPAA Security Rule requirements over the Avaamo Conversational AI platform to be achieved solely by Avaamo. Therefore, user entity controls must be evaluated in conjunction with Avaamo's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Avaamo periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports
- Regular meetings to discuss performance
- Non-disclosure agreements

| Control Activity Expected to be Implemented by Subservice Organizations | Subservice Organizations | Applicable Trust Services Criteria and HIPAA Security Rule Requirements |
|---|---|---|
| Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate. | Amazon Web Service | CC6.1, CC6.2, CC6.3, CC6.5, CC7.2 |
| Physical access to the data center facility is restricted to authorized personnel. | Amazon Web Services, GitHub, OpenVPN | CC6.4, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii) |
| Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements. | Amazon Web Services, GitHub, OpenVPN | CC6.5, A1.2, 164.310(a)(2)(ii) |
| Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically. | Amazon Web Services, GitHub, OpenVPN | A1.3, 164.308(a)(7)(i), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), |
| Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components. | Amazon Web Services, GitHub, OpenVPN | 164.310(a)(2)(iv) |

| Control Activity Expected to be Implemented by Subservice Organizations | Subservice Organizations | Applicable Trust Services Criteria and HIPAA Security Rule Requirements |
|---|---|---|
| A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality. | Amazon Web Services, GitHub, OpenVPN | C1.1 |
| A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities. | Amazon Web Services, GitHub, OpenVPN | C1.2 |
| A defined Privacy Policy and terms of service are in effect for all information stored and processed within the systems. | Amazon Web Services, GitHub, OpenVPN | P1.1, P2.1, P3.1 |
| A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality. | Amazon Web Services | CC1.1, 164.312(a)(1) |

# 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), BARR Advisory, P.A. 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; and/or,
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 controls (e.g., periodic reviews of user access lists), BARR Advisory, P.A. inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

# Section IV

## Description of Criteria, Avaamo's Related Controls, and BARR Advisory, P.A.'s Tests of Controls and Results

# Avaamo Controls Mapped to the Security, Confidentiality, Availability, and Privacy Criteria

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| **1.0 – Common Criteria Related to Control Environment** | | |
| CC1.1 | HR-1, HR-2, IS-2, IS-3 | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. |
| CC1.2 | IS-1, RC-1 | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. |
| CC1.3 | IS-1, IS-2, IS-3, IS-4 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. |
| CC1.4 | HR-1, HR-2, IS-2, IS-3, IS-4, IS-5, IS-6, RC-1 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. |
| CC1.5 | IS-1, IS-2, IS-3, IS-4 | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. |
| **2.0 – Common Criteria Related to Information and Communication** | | |
| CC2.1 | RC-1, RC-3 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. |
| CC2.2 | IS-1, IS-2, IS-3, IS-4, IS-5, IS-6, OM-05, RC-3 | COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. |
| CC2.3 | IS-1, IS-3, IS-6, OM-02, OM-03, OM-05 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. |
| **3.0 – Common Criteria Related to Risk Assessment** | | |
| CC3.1 | IS-1, RC-1, RC-3 | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. |
| CC3.2 | RC-1, RC-2, RC-3 | 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. |

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| CC3.3 | AM-1, RC-1, RC-2 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. |
| CC3.4 | RC-1, RC-2, RC-3, RC-4 | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. |
| **4.0 – Common Criteria Related to Monitoring Activities** | | |
| CC4.1 | OM-01, RC-1, RC-2, RC-3, RC-4 | 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. |
| CC4.2 | RC-1, RC-2, RC-3, RC-4 | 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. |
| **5.0 – Common Criteria Related to Control Activities** | | |
| CC5.1 | IS-1, IS-3, RC-1, RC-3 | 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. |
| CC5.2 | IS-1, IS-3, RC-1 | COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. |
| CC5.3 | HR-2, IS-1, IS-3, RC-3 | COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. |
| **6.0 – Common Criteria Related to Logical and Physical Access** | | |
| CC6.1 | AC-01, AC-02, AC-03, AC-04, AC-05, AC-06, AC-07, AC-08, AC-09, AC-10, AM-1, CR-2, OM-06, SC-1, SC-2 | 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. |
| CC6.2 | AC-03, AC-05, AC-06, AC-07 | 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. |

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| CC6.3 | AC-01, AC-03, AC-06, AC-07, OM-06 | 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. |
| CC6.4 | N/A - See complementary subservice controls | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. |
| CC6.5 | AM-1, OM-04 | 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. |
| CC6.6 | AC-01, AC-02, AC-03, AC-04, AC-05, AC-08, CR-1, CR-2, OM-01, SC-1, SC-2, TV-2 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. |
| CC6.7 | AC-05, AC-08, AM-1, CM-1, CR-1, CR-2, OM-01, SC-1, SC-2, TV-2 | 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. |
| CC6.8 | AC-08, AM-1, CM-5, CM-6, CR-1, OM-01, TV-2 | The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. |
| **7.0 – Common Criteria Related to System Operations** | | |
| CC7.1 | AC-08, AM-1, CM-5, CM-6, OM-01, OM-02, TV-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. |
| CC7.2 | AM-1, OM-01, RC-3, TV-1, TV-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. |

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| CC7.3 | OM-01, OM-02, TV-1 | 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. |
| CC7.4 | BC-1, OM-01, OM-02, RC-2, TV-1 | The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. |
| CC7.5 | OM-01, OM-02 | The entity identifies, develops, and implements activities to recover from identified security incidents. |
| **8.0 – Common Criteria Related to Change Management** | | |
| CC8.1 | AC-09, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6 | The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. |
| **9.0 – Common Criteria Related to Risk Mitigation** | | |
| CC9.1 | OM-01, OM-02, RC-1, RC-3 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. |
| CC9.2 | IS-1, RC-1, RC-2 | The entity assesses and manages risks associated with vendors and business partners. |
| **Additional Criteria for Confidentiality** | | |
| C1.1 | AM-1, HR-2, IS-3, OM-06 | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. |
| C1.2 | AM-1, IS-3, OM-04, OM-06 | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. |
| **Additional Criteria for Availability** | | |
| A1.1 | BC-1, BC-2, BC-3, BC-4, OM-01 | 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. |
| A1.2 | BC-1, BC-2, BC-3, BC-4 | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. |
| A1.3 | BC-1 | The entity tests recovery plan procedures supporting system recovery to meet its objectives. |

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| **Additional Criteria for Privacy** | | |
| P1.1 | PR-01, PR-02, PR-03, PR-04 | The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. |
| P2.1 | OM-03, PR-01, PR-02, PR-03 | The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. |
| P3.1 | CR-2, PR-02, PR-04, PR-05 | Personal information is collected consistent with the entity's objectives related to privacy. |
| P3.2 | OM-03, PR-01, PR-02, PR-03, PR-04, PR-05 | For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy. |
| P4.1 | OM-03, OM-04, PR-04, PR-05 | The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. |
| P4.2 | BC-3, OM-03, OM-04, OM-06, PR-01, PR-05, RC-1 | The entity retains personal information consistent with the entity's objectives related to privacy. |
| P4.3 | OM-04 | The entity securely disposes of personal information to meet the entity's objectives related to privacy. |
| P5.1 | N/A - Avaamo has no direct relationship with data subjects. | The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy. |

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| P5.2 | N/A - Avaamo has no direct relationship with data subjects. | The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy. |
| P6.1 | PR-03 | The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. |
| P6.2 | PR-03, PR-08 | The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy. |
| P6.3 | PR-09 | The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy. |
| P6.4 | PR-05, RC-2 | The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary. |
| P6.5 | OM-05, PR-08, PR-09, PR-10 | The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such Notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy. |
| P6.6 | OM-02, PR-10 | The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy. |
| P6.7 | N/A - Avaamo has no direct relationship with data subjects. | The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy. |
| P7.1 | OM-03, OM-04, OM-06, PR-02, PR-04, PR-05 | The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy. |

| Criteria | Supporting Control | Criteria Description |
|---|---|---|
| P8.1 | IS-6, OM-04, OM-06, PR-02, PR-04 | The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner. |

# Avaamo Controls Mapped to the HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule (2013 HIPAA Omnibus Final Rule) establishes national standards to protect individuals' ePHI that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The table below includes a mapping of the HIPAA Security Rule to the SOC 2 controls included in this SOC 2 examination.

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| **CFR §164.308 – Administrative Safeguards** | | |
| 164.308(a)(1)(i) Security Management Process | CM-1, IS-3, IS-6, OM-02 | Implement policies and procedures to prevent, detect, contain, and correct security violations. |
| 164.308(a)(1)(ii)(A) Risk Analysis (R) | IS-3, RC-1, RC-2, TV-1 | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. |
| 164.308(a)(1)(ii)(B) Risk Management (R) | CM-6, RC-1, RC-2, RC-3 | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a). |
| 164.308(a)(1)(ii)(C) Sanction Policy (R) | HR-2, IS-3 | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. |
| 164.308(a)(1)(ii)(D) Information System Activity Review (R) | AC-07, OM-01, RC-3, RC-4 | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. |
| 164.308(a)(2) Assigned Security Responsibility | IS-1, IS-3 | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. |
| 164.308(a)(3)(i) Workforce Security | AC-03, AC-06, AC-07, IS-3 | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. |

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| 164.308(a)(3)(ii)(A) Authorization and/ or Supervision (A) | AC-03, AC-07, HR-1 | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. |
| 164.308(a)(3)(ii)(B) Workforce Clearance Procedures (A) | AC-07 | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. |
| 164.308(a)(3)(ii)(C) Termination Procedures (A) | AC-06, AC-07, IS-3 | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. |
| 164.308(a)(4)(i) Information Access Management | AC-03, AC-06, AC-07, IS-3 | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. |
| 164.308(a)(4)(ii)(A) Isolation Health Clearinghouse Functions (R) | N/A - Avaamo does not conduct healthcare clearinghouse functions. | If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. |
| 164.308(a)(4)(ii)(B) Access Authorization | AC-03, AC-04, IS-3 | Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. |
| 164.308(a)(4)(ii)(C) Access Establishment and Modification (A) | AC-03, AC-06, AC-07, IS-3 | Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. |
| 164.308(a)(5)(i) Security Awareness Training | IS-2 | Implement a security awareness and training program for all members of its workforce (including management). |
| 164.308(a)(5)(ii)(A) Security Reminders (A) | IS-2, IS-3 | Periodic security updates. |

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| 164.308(a)(5)(ii)(B) Protection from Malicious Software (A) | AC-01, AC-08, OM-01, TV-2 | Procedures for guarding against, detecting, and reporting malicious software. |
| 164.308(a)(5)(ii)(C) Log-in Monitoring (A) | AC-08, OM-01, OM-02 | Procedures for monitoring log-in attempts and reporting discrepancies. |
| 164.308(a)(5)(ii)(D) Password Management (A) | AC-04, AC-10, IS-3 | Procedures for creating, changing, and safeguarding passwords. |
| 164.308(a)(6)(i) Security Incident Procedures | OM-01, OM-02 | Implement policies and procedures to address security incidents. |
| 164.308(a)(6)(ii) Response and Reporting (R) | OM-01, OM-02, RC-1, RC-2, RC-3, TV-1 | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. |
| 164.308(a)(7)(i) Contingency Plan | BC-1, BC-2, IS-2 | Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. |
| 164.308(a)(7)(ii)(A) Data Backup Plan (R) | BC-1, BC-2 | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. |
| 164.308(a)(7)(ii)(B) Disaster Recovery Plan (R) | BC-1, BC-2 | Establish (and implement as needed) procedures to restore any loss of data. |
| 164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (R) | BC-1, BC-2 | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. |
| 164.308(a)(7)(ii)(D) Testing and Revision Procedures (A) | BC-1, BC-2 | Implement procedures for periodic testing and revision of contingency plans. |
| 164.308(a)(7)(ii)(E) Application and Data Criticality Analysis (A) | BC-1, RC-1 | Assess the relative criticality of specific applications and data in support of other contingency plan components. |

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| | | |
| 164.308(a)(8) Evaluation | OM-03, OM-05, RC-1, RC-2 | Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. |
| 164.308(b)(1) and 164.308(b)(2) Business Associate Contracts and Other Arrangements | OM-03, OM-05 | (b)(1) A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.<br>(b)(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information. |
| 164.308(b)(3) Written Contract (R) | OM-03, OM-05 | Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a). |
| **CFR §164.310 – Physical Safeguards** | | |
| 164.310(a)(1) Facility Access Controls | All infrastructure supporting the Avaamo Conversational AI platform is housed in AWS. Please refer to CSOCs. | Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. |

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| 164.310(a)(2)(i) Contingency Operations (A) | All infrastructure supporting the Avaamo Conversational AI platform is housed in AWS. Please refer to CSOCs. | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. |
| 164.310(a)(2)(ii) Facility Security Plan (A) | All infrastructure supporting the Avaamo Conversational AI platform is housed in AWS. Please refer to CSOCs. | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. |
| 164.310(a)(2)(iii) Access Control Validation Procedures (A) | All infrastructure supporting the Avaamo Conversational AI platform is housed in AWS. Please refer to CSOCs. | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. |
| 164.310(a)(2)(iv) Maintenance Records (A) | All infrastructure supporting the Avaamo Conversational AI platform is housed in AWS. Please refer to CSOCs. | Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). |
| 164.310(b) Workstation Use | HR-2, IS-3 | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. |
| 164.310(c) Workstation Security | AC-04, TV-2 | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. |

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| 164.310(d)(1) Device and Media Controls | HR-2, IS-3 | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. |
| 164.310(d)(2)(i) Disposal (R) | OM-04 | Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. |
| 164.310(d)(2)(ii) Media Re-use (R) | OM-04 | Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. |
| 164.310(d)(2)(iii) Accountability (A) | AM-1, OM-04 | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. |
| 164.310(d)(2)(iv) Data Backup and Storage (A) | BC-3, CR-2, OM-04 | Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. |
| **CFR §164.312 – Technical Safeguards** | | |
| 164.312(a)(1) Access Control | AC-01, AC-02, AC-03, AC-04, AC-05, AC-09 | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). |
| 164.312(a)(2)(i) Unique User Identification (R) | AC-01, AC-02 | Assign a unique name and/or number for identifying and tracking user identity. |
| 164.312(a)(2)(ii) Emergency Access Procedure (R) | BC-1, OM-02 | Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. |
| 164.312(a)(2)(iii) Automatic Logoff (A) | AC-04 | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. |
| 164.312(a)(2)(iv) Encryption and Decryption (Stored) (A) | CR-1, CR-2 | Implement a mechanism to encrypt and decrypt electronic protected health information. |

| Criteria | Supporting Control | Safeguard Description |
|---|---|---|
| 164.312(b) Audit Controls | BC-4, OM-01, OM-02, RC-4 | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. |
| 164.312(c)(1) Integrity | AC-09, CR-1, CR-2, OM-02, OM-04, RC-4 | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. |
| 164.312(c)(2) Mechanism to Authenticate ePHI (A) | AC-02, AC-04, AC-05, AC-08 | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. |
| 164.312(d) Person or Entity Authentication | AC-03, AC-04, AC-05 | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. |
| 164.312(e)(1) Transmission Security | AC-02, AC-05, CR-1 | Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. |
| 164.312(e)(2)(i) Integrity Controls (A) | AC-02, CR-1, OM-04 | Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. |
| 164.312(e)(2)(ii) Encryption (Transmission) (A) | AC-02, CR-1, CR-2 | Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. |

# Security, Confidentiality, Availability, and Privacy Criteria and HIPAA Security Rule Mapped to Avaamo Controls, BARR Advisory, P.A.'s Tests, and Test Results

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| AC-01 | Access to systems requires a unique ID to establish accountability with user logins. | 164.308(a)(5)(ii)(B)<br>164.312(a)(1)<br>164.312(a)(2)(i)<br>CC6.1<br>CC6.3<br>CC6.6 | Inquired of management and inspected the Access Control Policy and system-generated user access lists for systems listed in Primary Infrastructure and Software table to determine if access to systems required a unique user ID to establish accountability with user logins.<br><br>**No exceptions noted.** |
| AC-02 | Administrator access is restricted to authorized system and security administrators. SSH protocol is used by administrators to authenticate with administrator access rights to the infrastructure. | 164.312(a)(1)<br>164.312(a)(2)(i)<br>164.312(c)(2)<br>164.312(e)(1)<br>164.312(e)(2)(i)<br>164.312(e)(2)(ii)<br>CC6.1<br>CC6.6 | Inquired of management and inspected the Access Control Policy and system-generated user access lists for systems listed in Primary Infrastructure and Software table to determine if administrator access was restricted to authorized system and security administrators.<br><br>Inspected the authentication protocol used by administrator accounts and observed a remote login session to determine if administrator access to the infrastructure required SSH.<br><br>**No exceptions noted.** |
| AC-03 | User access is approved by management in accordance with the Access Control Policy based on least privilege access principles. | 164.308(a)(3)(i)<br>164.308(a)(3)(ii)(A)<br>164.308(a)(4)(i)<br>164.308(a)(4)(ii)(B)<br>164.308(a)(4)(ii)(C)<br>164.312(a)(1)<br>164.312(d)<br>CC6.1<br>CC6.2<br>CC6.3<br>CC6.6 | Inquired of management and inspected the Access Control Policy and a selection of new or transferred users to determine if access was approved by management and provisioned based on least privilege access principles.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| AC-04 | User IDs with passwords are established on critical systems and applications to enforce:<br>• Eight character minimum;<br>• Six failed login attempts allowed before an account is locked out;<br>• Passwords expire annually if MFA is not established; and,<br>• Accounts are automatically logged out after a defined period of inactivity. | 164.308(a)(4)(ii)(B)<br>164.308(a)(5)(ii)(D)<br>164.310(c)<br>164.312(a)(1)<br>164.312(a)(2)(iii)<br>164.312(c)(2)<br>164.312(d)<br>CC6.1<br>CC6.6 | Inquired of management and inspected the Access Control Policy and password configuration settings for systems listed in Primary Infrastructure and Software table to determine if user IDs with passwords enforced an eight-character minimum, six failed login attempts allowed before an account is locked out, password expiration if MFA was not possible, and automatic account logouts after a defined period of inactivity.<br><br>**No exceptions noted.** |
| AC-05 | Access to cloud services systems and administrator accounts require multi-factor authentication where the user must enter a verification code in addition to their username and password upon sign in. | 164.312(a)(1)<br>164.312(c)(2)<br>164.312(d)<br>164.312(e)(1)<br>CC6.1<br>CC6.2<br>CC6.6<br>CC6.7 | Inquired of management and inspected the Access Control Policy and authentication settings for cloud services systems and administrator accounts to determine if MFA was enforced.<br><br>Observed a remote login session to determine if MFA was required.<br><br>**No exceptions noted.** |
| AC-06 | Terminated user access to production systems, tools, and the network is removed within 12 hours upon termination. | 164.308(a)(3)(i)<br>164.308(a)(3)(ii)(C)<br>164.308(a)(4)(i)<br>164.308(a)(4)(ii)(C)<br>CC6.1<br>CC6.2<br>CC6.3 | Inquired of management and inspected the System Access Control Policy and offboarding tickets for a sample of terminations to determine if access to production systems, tools, and the network was removed within 12 hours upon termination.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| AC-07 | User profile and access reviews are performed annually on all end-user and system-level accounts. The review includes a review of all active users, including employees and contractors. Access issues, if any, are resolved. | 164.308(a)(1)(ii)(D)<br>164.308(a)(3)(i)<br>164.308(a)(3)(ii)(A)<br>164.308(a)(3)(ii)(B)<br>164.308(a)(3)(ii)(C)<br>164.308(a)(4)(i)<br>164.308(a)(4)(ii)(C)<br>CC6.1<br>CC6.2<br>CC6.3 | Inquired of management and inspected the Access Control Policy to determine if user profile and access reviews were to be performed at least annually.<br><br>Inspected the most recent annual user access review for systems listed in Primary Infrastructure and Software table to determine if a review was performed at least annually over the following systems and access issues, if any, were resolved.<br><br>**No exceptions noted.** |
| AC-08 | Approved configuration standards exist for secure images and templates for operating systems and software. Entity security configuration standards are applied through automated deployment mechanisms to help ensure consistent application. | 164.308(a)(5)(ii)(B)<br>164.308(a)(5)(ii)(C)<br>164.312(c)(2)<br>CC6.1<br>CC6.6<br>CC6.7<br>CC6.8<br>CC7.1 | Inquired of management, inspected infrastructure-related policies, and Avaamo's configuration standards to determine if approved configuration standards existed for secure images and templates for operating systems and software.<br><br>Inspected hardening logs to determine if configuration standards were applied through automated deployment mechanisms within change management processes.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| AC-09 | Access to migrate change to production is restricted to authorized personnel. Code management tools force branch protection to help ensure users cannot bypass standard change controls. | 164.312(a)(1)<br>164.312(c)(1)<br>CC6.1<br>CC8.1 | Inquired of management and inspected the Change Management Policy and a system-generated list of users with access to production to determine if access to migrate software and configuration changes was restricted to authorized personnel.<br><br>Inspected code management tools to determine if branch protection settings were enforced that restricted users from bypassing standard changes controls.<br><br>**No exceptions noted.** |
| AC-10 | Access keys are rotated every 90 days for accounts with keys established. | 164.308(a)(5)(ii)(D)<br>CC6.1 | Inquired of management and inspected the Access Control Policy and key rotation documentation to determine if access keys were rotated at least every 90 days.<br><br>**No exceptions noted.** |
| AM-1 | Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. | 164.310(d)(2)(iii)<br>C1.1<br>C1.2<br>CC3.3<br>CC6.1<br>CC6.5<br>CC6.7<br>CC6.8<br>CC7.1<br>CC7.2 | Inquired of management and inspected the Asset Management Policy and current asset inventories to determine if assets used in the system were inventoried or tagged to include business descriptions, ownership, versions, and patch levels in accordance with policy.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| BC-1 | Contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents and testing. The contingency plan is tested on at least an annual basis. | 164.308(a)(7)(i)<br>164.308(a)(7)(ii)(A)<br>164.308(a)(7)(ii)(B)<br>164.308(a)(7)(ii)(C)<br>164.308(a)(7)(ii)(D)<br>164.308(a)(7)(ii)(E)<br>164.310(a)(2)(i)<br>164.312(a)(2)(ii)<br>A1.1<br>A1.2<br>A1.3<br>CC7.4 | Inquired of management and inspected the contingency plan and incident response plan to determine if contingency planning and incident response playbooks were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents and testing.<br><br>Inspected documentation for the most recent contingency plan test to determine if the contingency plan was tested within the past year.<br><br>**No exceptions noted.** |
| BC-2 | Critical system components are replicated across multiple availability zones to permit the resumption of critical operations in the event of loss of a critical facility. | 164.308(a)(7)(i)<br>164.308(a)(7)(ii)(A)<br>164.308(a)(7)(ii)(B)<br>164.308(a)(7)(ii)(C)<br>164.308(a)(7)(ii)(D)<br>164.310(a)(2)(i)<br>A1.1<br>A1.2 | Inquired of management and inspected the Information Security Policy and system configuration settings to determine if production environments were configured to replicate across multiple availability zones.<br><br>**No exceptions noted.** |
| BC-3 | Backups of critical system components are performed at least daily. Failed backups are monitored for successful replication. | 164.310(d)(2)(iv)<br>A1.1<br>A1.2<br>P4.2 | Inquired of management and inspected the Backup Policy and backup configurations to determine if at least daily backups were enabled.<br><br>Inspected the configurations to determine if backup failures automatically notified operations personnel in the event of a failure that would invoke incident management processes for monitoring of successful backups.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| BC-4 | Processing capacity is monitored through automated tools that alert operations. Issues, if any, are resolved through incident management processes. | 164.312(b)<br>A1.1<br>A1.2 | Inquired of management and inspected the Information Security Policy and real-time monitoring applications to determine if processing capacity issues in the production environment were continuously monitored.<br><br>Inspected the monitoring tool configurations to determine if processing capacity issues were automatically logged and tracked in the operations incident management systems.<br><br>**No exceptions noted.** |
| CM-1 | Change management policies are in place that include procedures for tracking, testing, and approving changes. Changes are tracked within change management or deployment tools. | 164.308(a)(1)(i)<br>164.310(a)(2)(iv)<br>CC6.7<br>CC8.1 | Inquired of management and inspected the Change Management Policy and a selection of changes to determine if change management policies were in place that included procedures for tracking, testing, and approving changes and if changes were tracked within change management or deployment tools.<br><br>**No exceptions noted.** |
| CM-2 | Change control, as defined by policy, requires approval and a peer review prior to implementation to help ensure change requirements are met and security issues are resolved. | CC8.1 | Inquired of the management and inspected the Change Management Policy and a selection of changes to determine if a peer review and approval was performed in accordance with the Change Management Policy prior to implementation.<br><br>**No exceptions noted.** |
| CM-3 | Changes are tested according to the nature of the change in an environment separate from production prior to deployment into a production release. | CC8.1 | Inquired of management and inspected the Change Management Policy and a selection of changes to determine if changes were tested in an environment separate from production prior to deployment.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| CM-4 | Customer content and personal information is not used in test and development environments. | CC8.1 | Inquired of management and inspected the Change Management Policy and different development environments to determine if personal information was not used in test and development environments.<br><br>**No exceptions noted.** |
| CM-5 | Software update tools are used to help ensure the operating systems are running the most recent security updates approved by management. | CC6.8<br>CC7.1<br>CC8.1 | Inquired of management and inspected the Threat and Vulnerability Management Policy, patch management configurations, and a selection of patches to determine if operating systems were updated in accordance with Avaamo-approved patch updates.<br><br>**No exceptions noted.** |
| CM-6 | Change management includes the application of static analysis tools prior to any production release to verify that secure coding practices are followed. Vulnerabilities identified, if any, are tracked to resolution. | 164.308(a)(1)(ii)(B),<br>CC6.8<br>CC7.1<br>CC8.1 | Inquired of management and inspected the Change Management Policy and a selection of releases to determine if static analysis tools were used to verify secure coding practices were followed and vulnerabilities, if any, were resolved.<br><br>**No exceptions noted.** |
| CR-1 | Strong cryptography and security protocols, such as TLS, SSH, or IPsec, are enforced to safeguard sensitive data during transmission over open, public networks. | 164.312(a)(2)(iv)<br>164.312(c)(1)<br>164.312(e)(1)<br>164.312(e)(2)(i)<br>164.312(e)(2)(ii)<br>CC6.6<br>CC6.7<br>CC6.8 | Inquired of management and inspected the Information Security Policy and cryptography and security protocols to determine if strong encryption was used for transmission over open, public networks.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| CR-2 | Strong cryptography standards for the storage of data are enforced in accordance with Data Classification and Handling Policy and customer commitments. | 164.310(a)(2)(iv)<br>164.310(d)(2)(iv)<br>164.312(a)(2)(iv)<br>164.312(c)(1)<br>164.312(e)(2)(ii)<br>CC6.1<br>CC6.6<br>CC6.7<br>P3.1 | Inquired of management, inspected the Data Classification and Handling Policy, a standard customer agreement, and encryption settings in place for resources with stored data to determine if strong cryptography standards were enforced in accordance with policy and customer commitments.<br><br>**No exceptions noted.** |
| HR-1 | Background or verification checks are performed on Avaamo personnel within 10 business days from hire date, as permitted by local laws | 164.308(a)(3)(ii)(A)<br>CC1.1<br>CC1.4 | Inquired of management and inspected the Personnel Security Policy and a selection of new hires to determine if background checks were performed within 10 business days from hire in accordance with policy and as permitted by local laws.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| HR-2 | Personnel are required to read and accept the Code of Conduct and statement of confidentiality during onboarding. Sanction policies are enacted for personnel who violate the code of conduct. | 164.308(a)(1)(ii)(C)<br>164.310(a)(2)(iii)<br>164.310(b)<br>164.310(d)(1)<br>C1.1<br>CC1.1<br>CC1.4<br>CC5.3 | Inquired of management and inspected the Personnel Security Policy to determine if personnel were required to read and accept the code of conduct and statement of confidentiality during onboarding and when the documents are modified and included sanction procedures.<br><br>Inspected a selection of new hires to determine if the Code of Conduct and statement of confidentiality were signed upon hire.<br><br>Inquired of management and was informed no personnel violated the Code of Conduct during the testing period.<br><br>**No exceptions noted.**<br><br>Inquired of management and determined no changes were made to the onboarding documents during the audit period and current employees were not required to reaffirm their understanding of these documents. **Therefore, this portion of the control did not take place and no conclusion was reached regarding its effectiveness.** |
| IS-1 | A security management plan defines the security governance team, with members independent of internal control along with security roles and responsibilities approved by the security committee or CISO-equivalent role. | 164.308(a)(2)<br>CC1.2<br>CC1.3<br>CC1.5<br>CC2.2<br>CC2.3<br>CC3.1<br>CC5.1<br>CC5.2<br>CC5.3<br>CC9.2 | Inquired of management, inspected the information security management policies to determine if an information security function with defined security roles and responsibilities was documented, approved, and included members independent from control operators.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| IS-2 | Avaamo maintains training programs to promote awareness of information security and HIPAA requirements as defined in the Security Awareness Policy. Trainings are conducted for all employees within 30 days of hire and each year thereafter. | 164.308(a)(5)(i)<br>164.308(a)(5)(ii)(A)<br>164.308(a)(7)(i)<br>CC1.1<br>CC1.3<br>CC1.4<br>CC1.5<br>CC2.2 | Inquired of management and inspected the Avaamo Awareness and Training Policy and a selection of new and current employees to determine if trainings were conducted for employees within 30 days of hire and annually thereafter to promote awareness of information security and HIPAA requirements.<br><br>**No exceptions noted.** |
| IS-3 | Information security policies are approved by management at least annually and published on internal collaboration tools accessible to all personnel with access to Avaamo systems. | 164.308(a)(1)(i)<br>164.308(a)(1)(ii)(A)<br>164.308(a)(1)(ii)(C)<br>164.308(a)(2)<br>164.308(a)(3)(i)<br>164.308(a)(3)(ii)(C)<br>164.308(a)(4)(i)<br>164.308(a)(4)(ii)(B)<br>164.308(a)(4)(ii)(C)<br>164.308(a)(5)(ii)(A)<br>164.308(a)(5)(ii)(D)<br>164.310(b)<br>164.310(d)(1)<br>C1.1<br>C1.2<br>CC1.1<br>CC1.3<br>CC1.4<br>CC1.5<br>CC2.2<br>CC2.3<br>CC5.1<br>CC5.2<br>CC5.3 | Inquired of management and inspected information security policies to determine if the policies were approved by management in the past year and published on internal collaboration tools accessible to Avaamo personnel.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| IS-4 | Avaamo has defined structures and reporting lines with assigned authority and responsibilities to meet business requirements. Avaamo performs formal evaluations at least annually of resourcing and staffing including assessment of employee qualification alignment with entity objectives. | CC1.3<br>CC1.4<br>CC1.5<br>CC2.2 | Inquired of management and inspected the organizational chart to determine if Avaamo had defined structures and reporting lines with assigned authority and responsibilities to meet business requirements.<br><br>Inspected a selection of current employees to determine if Avaamo performed formal evaluations at least annually, including assessment of employee qualification alignment with entity objectives.<br><br>**No exceptions noted.** |
| IS-5 | Avaamo maintains internal informational websites describing the system environment, its boundaries, user responsibilities, and services. System documentation includes security and hardening guides to help ensure effective configuration, installation, and operation of the information system. | CC1.4<br>CC2.2 | Inquired of management and inspected internal system documents and security hardening benchmarks posted on internal collaboration tools to determine if the system environment, its boundaries, user responsibilities, services, and security baselines were maintained and made available to internal users.<br><br>**No exceptions noted.** |
| IS-6 | Descriptions of the system and its boundaries are available to external users via ongoing communications with customers, official blog posts, and status portals. Customer incidents, if any, are reported and resolved through one-to-one communication via the customer ticketing system. | 164.308(a)(1)(i)<br>CC1.4<br>CC2.2<br>CC2.3<br>P8.1 | Inquired of management and inspected the Incident Management Policy and customer communications to determine if descriptions of the system and its boundaries were available to external users via ongoing communications with customers, official blog posts, and status portals.<br><br>Inspected a selection of customer incidents to determine if the incidents were resolved as defined in accordance with Avaamo policy.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| OM-01 | Monitoring and alarming are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Incidents, if any, are routed through incident management for resolution. | 164.308(a)(1)(ii)(D)<br>164.308(a)(5)(ii)(B)<br>164.308(a)(5)(ii)(C)<br>164.308(a)(6)(i)<br>164.308(a)(6)(ii)<br>164.312(b)<br>A1.1<br>CC4.1<br>CC6.6<br>CC6.7<br>CC6.8<br>CC7.1<br>CC7.2<br>CC7.3<br>CC7.4<br>CC7.5<br>CC9.1 | Inquired of management and inspected the Incident Management Policy and monitoring and alarming tool configurations to determine if security and operational metrics were monitored with predefined thresholds and if tools were configured to notify management automatically when thresholds were crossed.<br><br>Inspected a selection of incidents to determine incidents, if any, were routed through incident management for resolution.<br><br>**No exceptions noted.** |
| OM-02 | Policy and procedure documentation for incident management, which includes the responsibility and escalation levels for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are made available to internal and external users. | 164.308(a)(1)(i)<br>164.308(a)(5)(ii)(C)<br>164.308(a)(6)(i)<br>164.308(a)(6)(ii)<br>164.312(a)(2)(ii)<br>164.312(b)<br>164.312(c)(1)<br>CC2.3<br>CC7.1<br>CC7.3<br>CC7.4<br>CC7.5<br>CC9.1<br>P6.6 | Inquired of management and inspected incident response policies and procedures to determine if they included responsibilities and escalation levels for reporting operational failures, security incidents, system problems, and user complaints.<br><br>Inspected evidence of communication of the incident response policies and procedures to determine if the documents were made available to internal and external users.<br><br>**No exceptions noted.** |
| OM-03 | Standard service agreements between customers define service levels, when applicable, rules of use, and additional terms for governing each service product. | 164.308(a)(8)<br>164.308(b)(1)<br>164.308(b)(3)<br>CC2.3<br>P2.1<br>P3.2<br>P4.1<br>P4.2<br>P7.1 | Inquired of management and inspected a selection of customers to determine if standard service agreements were in place with defined service levels, rules of use, and additional terms for governing each service product.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| OM-04 | Customer data is disposed of in accordance with requirements defined within the Data Classification Policy. | 164.310(d)(2)(i)<br>164.310(d)(2)(ii)<br>164.310(d)(2)(iii)<br>164.310(d)(2)(iv)<br>164.312(c)(1)<br>164.312(e)(2)(i)<br>C1.2<br>CC6.5<br>P4.1<br>P4.2<br>P4.3<br>P7.1<br>P8.1 | Inquired of management and inspected the Data Classification and Handling Policy to determine if a process was in place for the disposal of customer data.<br><br>Inspected a selection of data deletion requests to determine if customer data was disposed of in accordance with the requirements defined within policy.<br><br>**No exceptions noted.** |
| OM-05 | Avaamo establishes agreements, including non-disclosure agreements and HIPAA BAAs, for preserving confidentiality and privacy of information and software exchanges with external parties. | 164.308(a)(8)<br>164.308(b)(1)<br>164.308(b)(3)<br>CC2.2<br>CC2.3<br>P6.5 | Inquired of management and inspected a selection of customers and a third-party vendor to determine if non-disclosure agreements and HIPAA BAAs were in place, as applicable, for preserving confidentiality and privacy of information and software exchanges with external parties.<br><br>**No exceptions noted.** |
| OM-06 | A Data Classification and Handling Policy is defined, reviewed, and approved on an annual basis. | C1.1<br>C1.2<br>CC6.1<br>CC6.3<br>P4.2<br>P7.1<br>P8.1 | Inquired of management and inspected the Data Classification and Handling Policy to determine if a Data Classification and Handling Policy was defined, reviewed, and approved on an annual basis.<br><br>**No exceptions noted.** |
| PR-01 | Avaamo has a Privacy Policy published on its website where it communicates its procedures in regards to the notice, choice and consent, collection, use, retention, disclosure, and disposal of personal information. | P1.1<br>P2.1<br>P3.2<br>P4.2 | Inquired of management and inspected Avaamo's Privacy Policy to determine if Avaamo had established a Privacy Policy, it was reviewed at least annually, and it defined procedures in regards to the notice, choice and consent, collection, use, retention, disclosure, and disposal of personal information.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| PR-02 | Avaamo informs customers of its security and privacy commitments within the terms of use and customer agreements and makes it available to customers to review at any time on the Avaamo website. | P1.1<br>P2.1<br>P3.1<br>P3.2<br>P7.1<br>P8.1 | Inquired of management and inspected the company's terms of use, customer agreements, and public-facing Privacy Policy to determine if Avaamo informed customers of its security and privacy commitments.<br><br>**No exceptions noted.** |
| PR-03 | Users of the system acknowledge that they've read the privacy commitments which include consenting to the collection, use, retention, disclosure, and disposal of personal information which are described within the master service agreements. | P1.1<br>P2.1<br>P3.2<br>P6.1<br>P6.2 | Inquired of management and inspected a selection of customers to determine if users of the system acknowledged that they've read the privacy commitments which included consenting to the collection, use, retention, disclosure, and disposal of personal information as described within the master service agreements.<br><br>**No exceptions noted.** |
| PR-04 | Avaamo communicates its objectives related to privacy within the master service agreements and Privacy Policy which are made available on the website. | P1.1<br>P3.1<br>P3.2<br>P4.1<br>P7.1<br>P8.1 | Inquired of management and inspected the company's master service agreements and Privacy Policy to determine if Avaamo communicated its objectives related to privacy.<br><br>**No exceptions noted.** |
| PR-05 | Personal information is collected consistent with the organization's privacy commitments and system requirements. | P3.1<br>P3.2<br>P4.1<br>P4.2<br>P6.4<br>P7.1 | Inquired of management and inspected the data processing agreement, Compliance and Confidentiality Policy, and system configurations to determine if the personal information collected was consistent with the organization's privacy commitments and system requirements.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| PR-06 | Avaamo retains personal information consistent with its privacy commitments and as long as it is required for its intended purpose. | P4.2<br>P6.2<br>P6.3 | Inquired of management and inspected a selection of current and terminated customers records and associated privacy commitments to determine if the organization retained personal information consistent with its privacy commitments.<br><br>**No exceptions noted.** |
| PR-07 | Avaamo has a data subject request (DSR) process to provide data subjects with information upon request when identified and authenticated. If the organization is unable to identify and authenticate, rationale for the access denial is provided. | P8.1 | Inquired of management and inspected the data subject request process and a selection of data subject requests to determine if the company provided data subjects with information upon request when identified and authenticated and provided rationale for the denial of access as applicable.<br><br>**No exceptions noted.** |
| PR-08 | Avaamo records instances of authorized disclosures to meet the entity's objectives related to privacy. | P6.2<br>P6.5 | Inquired of management and inspected the company's Privacy Policy, Data Classification Policy, and data processing agreement to determine if procedures were in place around the recording of authorized disclosures.<br><br>Inspected a system-generated list of all Jira tickets during the period and determined that there were no Jira tickets related to authorized disclosures and as such, noted there were no authorized disclosures during the period. **Therefore, this control did not operate and no conclusion was reached regarding its operating effectiveness.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| PR-09 | Avaamo records instances of unauthorized disclosures to meet the entity's objectives related to privacy. | P6.3<br>P6.5 | Inquired of management and inspected the company's Privacy Policy, Data Classification Policy, and data processing agreement to determine if procedures were in place around the recording of unauthorized disclosures.<br><br>Inspected a system-generated list of Jira tickets and determined that there were no unauthorized disclosures during the period. **Therefore, this control did not operate and no conclusion was reached regarding its operating effectiveness.** |
| PR-10 | Avaamo provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy. | P6.5<br>P6.6 | Inquired of management and inspected the Information Security Incident Response Policy to determine if procedures were in place to govern the process of notifying affected data subjects and regulators of breaches and incidents as legally required and in accordance with team processes.<br>Inspected a system-generated list of incident tickets and determined there were no data breaches and incidents requiring notification to affected data subjects, regulators, and others during the reporting period. **Therefore, this control did not operate and no conclusion was reached regarding its operating effectiveness.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| RC-1 | Avaamo performs a formal risk assessment on an annual basis where relevant risks to the organization are identified and evaluated. Identified risks and mitigation strategies are documented within a centralized risk register. | 164.308(a)(1)(ii)(A)<br>164.308(a)(1)(ii)(B)<br>164.308(a)(6)(ii)<br>164.308(a)(7)(ii)(E)<br>164.308(a)(8)<br>CC1.2<br>CC1.4<br>CC2.1<br>CC3.1<br>CC3.2<br>CC3.3<br>CC3.4<br>CC4.1<br>CC4.2<br>CC5.1<br>CC5.2<br>CC9.1<br>CC9.2<br>P4.2 | Inquired of management and inspected the Risk Assessment Program Policy and annual risk assessment to determine if an annual risk assessment was performed, relevant risks to the organization were identified and evaluated, and mitigation strategies were documented within a centralized risk register.<br><br>**No exceptions noted.** |
| RC-2 | Third-party risk assessments are performed at least annually as part of the vendor risk management process. Attestation reports or business associate agreements are evaluated, when applicable. | 164.308(a)(1)(ii)(A)<br>164.308(a)(1)(ii)(B)<br>164.308(a)(6)(ii)<br>164.308(a)(8)<br>CC3.2<br>CC3.3<br>CC3.4<br>CC4.1<br>CC4.2<br>CC7.4<br>CC9.2<br>P6.4 | Inquired of management and inspected the Third-party Risk Management Policy and results of the most recent third-party risk assessments to determine if reviews were performed at least annually as part of the vendor risk management process and included reviews of attestation reports or business associate agreements, when applicable.<br><br>**No exceptions noted.** |
| RC-3 | Information security key performance indicators are defined and reviewed monthly for compliance status (i.e., SLAs, patch levels, security awareness compliance, high risk vulnerabilities, etc.). Metrics outside of defined thresholds have a documented remediation plan. | 164.308(a)(1)(ii)(B)<br>164.308(a)(1)(ii)(D)<br>164.308(a)(6)(ii)<br>CC2.1<br>CC2.2<br>CC3.1<br>CC3.2<br>CC3.4<br>CC4.1<br>CC4.2<br>CC5.1<br>CC5.3<br>CC7.2<br>CC9.1 | Inquired of management and inspected documented information security key performance indicators to determine if they were defined.<br><br>Inspected a selection of months to determine if information security key performance indicators were reviewed and metrics outside of defined thresholds had documented remediation plans.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| RC-4 | Independent internal control evaluations are performed at least annually against the ISMS objectives, service commitments, and compliance objectives. | 164.308(a)(1)(ii)(D)<br>164.312(b)<br>164.312(c)(1)<br>CC3.4<br>CC4.1<br>CC4.2 | Inquired of management and inspected internal control evaluations to determine if independent internal control evaluations were performed at least annually against the ISMS objectives, service commitments, and compliance objectives.<br><br>**No exceptions noted.** |
| SC-1 | Security groups are configured to enforce perimeter security including configurations that deny all traffic by default, restrict ingress traffic from sensitive protocols, and restrict authentication to infrastructure systems to trusted IP addresses. | CC6.1<br>CC6.6<br>CC6.7 | Inquired of management and inspected production security group configurations to determine if perimeter security was in place including:<br>• Default deny all traffic;<br>• Restricted ingress traffic from sensitive protocols; and,<br>• Restricted authentication to infrastructure systems to trusted IP addresses.<br><br>**No exceptions noted.** |
| SC-2 | WAFs are deployed to inspect traffic to the web application and prevent and log common web application attacks. | CC6.1<br>CC6.6<br>CC6.7 | Inquired of management and inspected WAF configurations to determine if a WAF was deployed to inspect traffic to the web application and prevent and log common web application attacks.<br><br>**No exceptions noted.** |

| No. | Description of Controls | Criteria | Tests of Controls and Test Results |
|---|---|---|---|
| TV-1 | External penetration testing is performed following each major release and at least annually. Issues are routed through incident and risk management processes for resolution. | 164.308(a)(1)(ii)(A)<br>164.308(a)(6)(ii)<br>CC7.1<br>CC7.2<br>CC7.3<br>CC7.4 | Inquired of management and inspected the Threat and Vulnerability Policy and results of the most recent penetration test to determine if it was performed within the last year by an external party.<br><br>Inspected evidence of management review including risk and incident tracking to determine issues, if any, were routed through incident and risk management processes for resolution.<br><br>**No exceptions noted.** |
| TV-2 | Avaamo end-user protection mechanisms include mobile device management (MDM) enforced on devices used to support the Avaamo Conversational AI platform. MDM requirements include full-disk encryption and the ability to remotely wipe a lost or stolen device | 164.308(a)(5)(ii)(B)<br>164.310(a)(2)(iv)<br>164.310(c)<br>CC6.6<br>CC6.7<br>CC6.8<br>CC7.2 | Inquired of the management and inspected the Asset Management Policy and MDM settings to determine if devices used to support the Avaamo Conversational AI platform required full-disk encryption and the ability to remotely wipe a lost or stolen device.<br><br>**No exceptions noted.** |

# Section V

## Other Information Provided by Avaamo That is Not Covered by the Service Auditor's Report

# Additional Information Provided by Avaamo to Provide a Mapping of Avaamo Controls to Version 1.1 of the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF)

NIST worked with stakeholders to develop a voluntary framework, based on existing standards, guidelines, and practices, for reducing cyber risks to critical infrastructure. The Cybersecurity Enhancement Act of 2014 reinforced NIST's EO 13636 rule. Created through collaboration between industry and government, the voluntary framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity related risk.

The table below includes a mapping of the NIST CSF to the SOC 2 controls included in this SOC 2 examination.

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Identify (ID) Domain**<br>*Objective: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.* | | |
| **Asset Management (ID.AM)**<br>*Objective: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.* | | |
| ID.AM-1 | Physical devices and systems within the organization are inventoried. | AM-1 |
| ID.AM-2 | Software platforms and applications within the organization are inventoried. | AM-1 |
| ID.AM-3 | Organizational communication and data flows are mapped. | IS-5 |
| ID.AM-4 | External information systems are cataloged. | AM-1 |
| ID.AM-5 | Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value. | AM-1, BC-1 |
| ID.AM-6 | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. | IS-1, IS-4, RC-3 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Business Environment (ID.BE)**<br>*Objective: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.* | | |
| ID.BE-1 | The organization's role in the supply chain is identified and communicated. | IS-1, OM-03, RC-2, RC-3 |
| ID.BE-2 | The organization's place in critical infrastructure and its industry sector is identified and communicated. | IS-1, RC-1 |
| ID.BE-3 | Priorities for organizational mission, objectives, and activities are established and communicated. | IS-1, IS-3 |
| ID.BE-4 | Dependencies and critical functions for delivery of critical services are established. | BC-1, IS-1 |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations). | BC-1, IS-1, RC-1, RC-2 |
| **Governance (ID.GV)**<br>*Objective: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.* | | |
| ID.GV-1 | Organizational cybersecurity policy is established and communicated. | IS-1, IS-2 |
| ID.GV-2 | Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. | IS-1, IS-4 |
| ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. | IS-1, RC-1, PR-01, PR-02, PR-03, PR-04 |
| ID.GV-4 | Governance and risk management processes address cybersecurity risks. | RC-1, RC-2 |
| **Risk Assessment (ID.RA)**<br>*Objective: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.* | | |
| ID.RA-1 | Asset vulnerabilities are identified and documented. | TV-1, SC-2 |
| ID.RA-2 | Cyber threat intelligence is received from information sharing forums and sources. | IS-1, RC-1 |
| ID.RA-3 | Threats, both internal and external, are identified and documented. | RC-1 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| ID.RA-4 | Potential business impacts and likelihoods are identified. | RC-1 |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. | RC-1 |
| ID.RA-6 | Risk responses are identified and prioritized. | RC-1 |
| **Risk Management Strategy (ID.RM)**<br>*Objective: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.* | | |
| ID.RM-1 | Risk management processes are established, managed, and agreed to by organizational stakeholders. | IS-1, RC-1 |
| ID.RM-2 | Organizational risk tolerance is determined and clearly expressed. | IS-1, RC-1 |
| ID.RM-3 | The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis. | IS-1, RC-1 |
| **Supply Chain Risk Management (ID.SC)**<br>*Objective: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.* | | |
| ID.SC-1 | Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. | RC-1, RC-2 |
| ID.SC-2 | Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process. | RC-1, RC-2 |
| ID.SC-3 | Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and cyber supply chain risk management plan. | OM-03, RC-3 |
| ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | RC-2 |
| ID.SC-5 | Response and recovery planning and testing are conducted with suppliers and third-party providers. | BC-1, RC-3 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Protect Domain (PR)**<br>*Objective: Develop and implement appropriate safeguards to ensure delivery of critical services.* | | |
| **Identity Management, Authentication, and Access Control (PR.AC)**<br>*Objective: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.* | | |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. | AC-01, AC-03, AC-05, AC-06, AC-07, AC-09, AC-10 |
| PR.AC-2 | Physical access to assets is managed and protected. | All infrastructure supporting the Avaamo Conversational AI platform is housed in AWS. |
| PR.AC-3 | Remote access is managed. | AC-02 |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | AC-03, AC-08 |
| PR.AC-5 | Network integrity is protected (e.g., network segregation, network segmentation). | AC-08, SC-1 |
| PR.AC-6 | Identities are proofed and bound to credentials and asserted in interactions. | AC-01, AC-02, AC-05, AC-10 |
| PR.AC-7 | Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). | AC-02, AC-04 |
| **Awareness and Training (PR.AT)**<br>*Objective: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.* | | |
| PR.AT-1 | All users are informed and trained. | HR-2, IS-2, IS-5 |
| PR.AT-2 | Privileged users understand their roles and responsibilities. | IS-2, IS-3, IS-5 |
| PR.AT-3 | Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. | IS-6, OM-03 |
| PR.AT-4 | Senior executives understand their roles and responsibilities. | IS-1, IS-2 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| PR.AT-5 | Physical and cybersecurity personnel understand their roles and responsibilities. | IS-1, IS-2, IS-4, IS-5 |
| **Data Security (PR.DS)**<br>*Objective: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.* | | |
| PR.DS-1 | Data-at-rest is protected. | CR-2 |
| PR.DS-2 | Data-in-transit is protected. | CR-1 |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition. | AM-1, OM-04 |
| PR.DS-4 | Adequate capacity to ensure availability is maintained. | BC-4 |
| PR.DS-5 | Protections against data leaks are implemented. | SC-1, SC-2 |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity. | OM-01 |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment. | CM-1, CM-3 |
| PR.DS-8 | Integrity checking mechanisms are used to verify hardware integrity. | N/A - This control is managed by AWS. |
| **Information Protection Processes and Procedures (PR.IP)**<br>*Objective: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.* | | |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems are created and maintained incorporating security principles (e.g., concept of least functionality). | AC-08 |
| PR.IP-2 | A system development life cycle to manage systems is implemented. | CM-1 |
| PR.IP-3 | Configuration change control processes are in place. | AC-08, CM-1, TV-1 |
| PR.IP-4 | Backups of information are conducted, maintained, and tested. | BC-1, BC-2 |
| PR.IP-5 | Policy and regulations regarding the physical operating environment for organizational assets are met. | AM-1, IS-3 |
| PR.IP-6 | Data is destroyed according to policy. | IS-5, OM-04 |
| PR.IP-7 | Protection processes are improved. | RC-3, RC-4 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| PR.IP-8 | Effectiveness of protection technologies is shared. | RC-3, RC-4 |
| PR.IP-9 | Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) are in place and managed. | BC-1, OM-02 |
| PR.IP-10 | Response and recovery plans are tested. | BC-1 |
| PR.IP-11 | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). | AC-06, HR-1, IS-4 |
| PR.IP-12 | A vulnerability management plan is developed and implemented. | IS-3, SC-2, TV-1 |
| **Maintenance (PR.MA)**<br>*Objective: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.* | | |
| PR.MA-1 | Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. | AM-1, CM-5 |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | CM-1 |
| **Protective Technology (PR.PT)**<br>*Objective: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.* | | |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | OM-01, OM-02 |
| PR.PT-2 | Removable media is protected and its use is restricted according to policy. | HR-2, IS-3 |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | AC-02, AC-08 |
| PR.PT-4 | Communications and control networks are protected. | CR-1, SC-1 |
| PR.PT-5 | Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | BC-2, OM-01 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Detect Domain (DE)**<br>*Objective: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.* | | |
| **Anomalies and Events (DE.AE)**<br>*Objective: Anomalous activity is detected and the potential impact of events is understood.* | | |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems are established and managed. | AC-08, IS-5 |
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods. | OM-01, OM-02 |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors. | OM-01, SC-2 |
| DE.AE-4 | Impact of events is determined. | RC-1, SC-2 |
| DE.AE-5 | Incident alert thresholds are established. | OM-01 |
| **Security Continuous Monitoring (DE.CM)**<br>*Objective: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.* | | |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events. | OM-01, SC-1, SC-2 |
| DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events. | N/A - This control is managed by AWS. |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events. | OM-01 |
| DE.CM-4 | Malicious code is detected. | CM-6, OM-01, TV-1 |
| DE.CM-5 | Unauthorized mobile code is detected. | CM-6, OM-01, TV-1 |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events. | OM-01, RC-2 |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed. | OM-01, TV-1 |
| DE.CM-8 | Vulnerability scans are performed. | TV-1 |
| **Detection Processes (DE.DP)**<br>*Objective: TDetection processes and procedures are maintained and tested to ensure awareness of anomalous events.* | | |
| DE.DP-1 | Roles and responsibilities for detection are well defined to ensure accountability. | IS-1, IS-5 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| DE.DP-2 | Detection activities comply with all applicable requirements. | IS-3, OM-02, RC-4 |
| DE.DP-3 | Detection processes are tested. | BC-1 |
| DE.DP-4 | Event detection information is communicated. | OM-01, OM-02 |
| DE.DP-5 | Detection processes are continuously improved. | RC-1, RC-4 |
| **Respond Domain (RS)**<br>*Objective: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.* | | |
| **Response Planning (RS.RP)**<br>*Objective: Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.* | | |
| RS.RP-1 | Response plan is executed during or after an incident. | OM-01, OM-02 |
| **Communications (RS.CO)**<br>*Objective: Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).* | | |
| RS.CO-1 | Personnel know their roles and order of operations when a response is needed. | IS-5, OM-02, PR-02, PR-09, PR-10 |
| RS.CO-2 | Incidents are reported consistent with established criteria. | OM-02, PR-02, PR-09, PR-10 |
| RS.CO-3 | Information is shared consistent with response plans. | IS-6, OM-02, PR-02 |
| RS.CO-4 | Coordination with stakeholders occurs consistent with response plans. | IS-6, OM-02, PR-02 |
| RS.CO-5 | Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. | IS-6 |
| **Analysis (RS.AN)**<br>*Objective: Analysis is conducted to ensure effective response and support recovery activities.* | | |
| RS.AN-1 | Notifications from detection systems are investigated. | OM-01, OM-02 |
| RS.AN-2 | The impact of the incident is understood. | OM-01, OM-02 |
| RS.AN-3 | Forensics are performed. | OM-02 |
| RS.AN-4 | Incidents are categorized consistent with response plans. | OM-02 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| RS.AN-5 | Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers). | OM-02, RC-1 |
| **Mitigation (RS.MI)**<br>*Objective: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.* | | |
| RS.MI-1 | Incidents are contained. | OM-01, OM-02 |
| RS.MI-2 | Incidents are mitigated. | OM-02 |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks. | SC-2, TV-1 |
| **Improvements (RS.IM)**<br>*Objective: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.* | | |
| RS.IM-1 | Response plans incorporate lessons learned. | OM-02 |
| RS.IM-2 | Response strategies are updated. | IS-3, OM-02 |
| **Recover Domain (RC)**<br>*Objective: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.* | | |
| **Recovery Planning (RC.RP)**<br>*Objective: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.* | | |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident. | OM-02 |
| **Improvements (RC.IM)**<br>*Objective: Recovery planning and processes are improved by incorporating lessons learned into future activities.* | | |
| RC.IM-1 | Recovery plans incorporate lessons learned. | OM-02 |
| RC.IM-2 | Recovery strategies are updated. | IS-3, OM-02 |
| **Communications (RC.CO)**<br>*Objective: Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).* | | |
| RC.CO-1 | Public relations are managed. | OM-02, RC-1 |
| RC.CO-2 | Reputation is repaired after an incident. | OM-02, RC-1 |

| NIST Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| RC.CO-3 | Recovery activities are communicated to internal and external stakeholders as well as executive and management teams. | IS-1, IS-3, IS-6, OM-02, RC-1 |

# Additional Information Provided by Avaamo to Provide a Mapping of Avaamo Controls to the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) V4.0 Framework

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the CSA guidance in 13 domains. The foundations of the CCM rest on its customized relationship to other industry accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum, and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.

The table below includes a mapping of the CSA CCM V3.0 Framework to the SOC 2 controls included in this SOC 2 examination.

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Audit and Assurance** | | |
| A&A-01 | Establish, document, approve, communicate, apply, evaluate, and maintain audit and assurance policies, procedures, and standards. Review and update the policies and procedures at least annually. | IS-3 |
| A&A-02 | Conduct independent audit and assurance assessments according to relevant standards at least annually. | RC-1, RC-4 |
| A&A-03 | Perform independent audit and assurance assessments according to risk-based plans and policies. | RC-1, RC-4 |
| A&A-04 | Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. | RC-1, RC-4 |
| A&A-05 | Define and implement an audit management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence. | IS-3, RC-1, RC-4 |
| A&A-06 | Establish, document, approve, communicate, apply, evaluate, and maintain a risk-based corrective action plan to remediate audit findings, review, and report remediation status to relevant stakeholders. | RC-1, RC-4 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Application and Interface Security** | | |
| AIS-01 | Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery, and support of the organization's application security capabilities. Review and update the policies and procedures at least annually. | IS-1, IS-3 |
| AIS-02 | Establish, document, and maintain baseline requirements for securing different applications. | AC-08, IS-3 |
| AIS-03 | Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations. | OM-01, RC-3 |
| AIS-04 | Define and implement a software development lifecycle (SDLC) process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. | CM-1 |
| AIS-05 | Implement a testing strategy, including criteria for acceptance of new information systems, upgrades, and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible. | CM-2, CM-3, CM-6 |
| AIS-06 | Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible. | CM-1, CM-2, CM-3, CM-6 |
| AIS-07 | Define and implement a process to remediate application security vulnerabilities, automating remediation when possible. | CM-6, TV-1 |
| **Business Continuity Management and Operational Resilience** | | |
| BCR-01 | Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures.Review and update the policies and procedures at least annually. | BC-1 |
| BCR-02 | Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. | BC-1, RC-1 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| BCR-03 | Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite. | BC-1, RC-1 |
| BCR-04 | Establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities. | BC-1, BC-2, BC-3, BC-4 |
| BCR-05 | Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically. | BC-1, BC-2, BC-3, BC-4 |
| BCR-06 | Exercise and test business continuity and operational resilience plans at least annually or upon significant changes. | BC-1 |
| BCR-07 | Establish communication with stakeholders and participants in the course of business continuity and resilience procedures. | BC-1, IS-3 |
| BCR-08 | Periodically backup data stored in the cloud. Ensure the confidentiality, integrity, and availability of the backup, and verify data restoration from backup for resiliency. | BC-1, BC-2, BC-3, CR-2 |
| BCR-09 | Establish, document, approve, communicate, apply, evaluate, and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes. | BC-1 |
| BCR-10 | Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities. | BC-1 |
| BCR-11 | Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards. | BC-2, BC-3 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Change Control and Configuration Management** | | |
| CCC-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration,etc., regardless of whether the assets are managed internally or externally(i.e., outsourced). Review and update the policies and procedures at least annually. | CM-0, RC-01 |
| CCC-02 | Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards. | CM-02, CM-03, CM-06 |
| CCC-03 | Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc.,regardless of whether the assets are managed internally or externally (i.e.,outsourced). | CM-02, CM-03, CM-06, RC-01 |
| CCC-04 | Restrict the unauthorized addition, removal, update, and management of organization assets. | AC-02, AC-09, AM-01, CM-05 |
| CCC-05 | Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs. | OM-03 |
| CCC-06 | Establish change management baselines for all relevant authorized changes on organization assets. | CM-01, CM-02, CM-03, CM-06 |
| CCC-07 | Implement detection measures with proactive notification in case of changes deviating from the established baseline. | CM-01, CM-02, CM-03, CM-06 |
| CCC-08 | 'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.' | CM-01, CM-02 |
| CCC-09 | Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns. | CM-01 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| **Encryption and Key Management Policy and Procedures** | | |
| CEK-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually. | IS-03 |
| CEK-02 | Define and implement cryptographic, encryption and key management roles and responsibilities. | IS-01, IS-03 |
| CEK-03 | Provide cryptographic protection to data at-rest and in-transit,using cryptographic libraries certified to approved standards. | CR-01, CR-02 |
| CEK-04 | Use encryption algorithms that are appropriate for data protection,considering the classification of data, associated risks, and usability of the encryption technology. | CR-01, CR-02 |
| CEK-05 | Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes. | CM-01, CM-02, CM-03, CM-06 |
| CEK-06 | Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis. | CM-01, CM-02, CM-03, CM-06, IS-03 |
| CEK-07 | Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context,monitoring, and feedback. | RC-01 |
| CEK-08 | CSPs must provide the capability for CSCs to manage their own data encryption keys. | OM-03 |
| CEK-09 | Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s). | RC-02, IS-03 |
| CEK-10 | Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used. | CR-01, CR-02 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| CEK-11 | Manage cryptographic secret and private keys that are provisioned for a unique purpose. | CR-01, CR-02 |
| CEK-12 | Rotate cryptographic keys in accordance with the calculated cryptoperiod,which includes provisions for considering the risk of information disclosure and legal and regulatory requirements. | CR-01, CR-02, OM-03 |
| CEK-13 | Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-14 | Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-15 | Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-16 | Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-17 | Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-18 | Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-19 | Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstances,and thereafter exclusively for decrypting data and never for encrypting data,which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| CEK-20 | Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| CEK-21 | Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements. | CR-01, CR-02, IS-03 |
| **Datacenter Security** | | |
| DCS-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually. | AC-06, IS-03 |
| DCS-02 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software,or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization.Review and update the policies and procedures at least annually. | CM-03, HR-02, IS-06 |
| DCS-03 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually. | IS-03, HR-02 |
| DCS-04 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually. | IS-03, HR-02 |
| DCS-05 | Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. | AM-01 |
| DCS-06 | Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system. | AM-01 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| DCS-07 | Implement physical security perimeters to safeguard personnel, data,and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas. | IS-03, RC-02 |
| DCS-08 | Use equipment identification as a method for connection authentication. | AC-04, AC-05, AM-01 |
| DCS-09 | Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization. | AC-02, OM-01, SC-01, SC-02 |
| DCS-10 | Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts. | IS-03, RC-02 |
| DCS-11 | Train datacenter personnel to respond to unauthorized ingress or egress attempts. | RC-02 |
| DCS-12 | Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities,offices and rooms. | RC-02 |
| DCS-13 | Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards. | RC-02 |
| DCS-14 | Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals. | BC-01, RC-02 |
| DCS-15 | Keep business-critical equipment away from locations subject to high probability for environmental risk events. | BC-02, BC-03, RC-02 |
| **Data Security and Privacy Lifecycle Management** | | |
| DSP-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations,standards, and risk level. Review and update the policies and procedures at least annually. | OM-06 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| DSP-02 | Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means. | AC-06, OM-04 |
| DSP-03 | Create and maintain a data inventory, at least for any sensitive data and personal data. | AM-01, OM-06 |
| DSP-04 | Classify data according to its type and sensitivity level. | OM-06 |
| DSP-05 | Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals,at least annually, and after any change. | AM-01, OM-06 |
| DSP-06 | Document ownership and stewardship of all relevant documents personal and sensitive data. Perform review at least annually. | OM-06 |
| DSP-07 | Develop systems, products, and business practices based upon a principle of security by design and industry best practices. | IS-03 |
| DSP-08 | Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations. | IS-03, OM-06 |
| DSP-09 | Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices. | This control was not included in the scope of the SOC examination. |
| DSP-10 | Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations. | CR-01, IS-06, OM-06 |
| DSP-11 | Define and implement processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations. | OM-04 |
| DSP-12 | Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject. | IS-06, OM-06, PR-07 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| DSP-13 | Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations. | CR-01, IS-06, PR-07 |
| DSP-14 | Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing. | IS-06, OM-06, PR-07 |
| DSP-15 | Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments. | CM-04 |
| DSP-16 | Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations. | OM-04 |
| DSP-17 | Define and implement processes, procedures and technical measures to protect sensitive data throughout its lifecycle. | CR-01, CR-02, OM-01, OM-06 |
| DSP-18 | The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation. | IS-06 |
| DSP-19 | Define and implement processes, procedures and technical measures to specify and document the physical locations of data, including any location in which data is processed or backed up. | BC-02, BC-03, IS-03, OM-0 |
| **Governance, Risk and Compliance** | | |
| GRC-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually. | IS-03, RC-01 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| GRC-02 | Establish a formal, documented, and leadership-sponsored EnterpriseRisk Management (ERM) program that includes policies and procedures for identification,evaluation, ownership, treatment, and acceptance of cloud security and privacy risks. | RC-01 |
| GRC-03 | Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization. | IS-03 |
| GRC-04 | Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs. | IS-03 |
| GRC-05 | Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM. | IS-03 |
| GRC-06 | Define and document roles and responsibilities for planning, implementing,operating, assessing, and improving governance programs. | IS-03 |
| GRC-07 | Identify and document all relevant standards, regulations, legal/contractual,and statutory requirements, which are applicable to your organization. | IS-03 |
| GRC-08 | Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context. | BC-03 |
| **Human Resources** | | |
| HRS-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually. | HR-01 |
| HRS-02 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually. | IS-03 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| HRS-03 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually. | IS-03 |
| HRS-04 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually. | IS-03 |
| HRS-05 | Establish and document procedures for the return of organization-owned assets by terminated employees. | IS-03 |
| HRS-06 | Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment. | HR-02, IS-03 |
| HRS-07 | Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets. | HR-02 |
| HRS-08 | The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies. | HR-02, IS-03 |
| HRS-09 | Document and communicate roles and responsibilities of employees,as they relate to information assets and security. | IS-01, IS-03 |
| HRS-10 | Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details. | HR-02, IS-03 |
| HRS-11 | Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates. | IS-02 |
| HRS-12 | Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization. | IS-02 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| HRS-13 | Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. | HR-02, IS-02 |
| **Identity & Access Management** | | |
| IAM-01 | Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually. | AC-02, AC-07, IS-03 |
| IAM-02 | Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually. | AC-04, AC-05 |
| IAM-03 | Manage, store, and review the information of system identities, and level of access. | AC-02, AC-07 |
| IAM-04 | Employ the separation of duties principle when implementing information system access. | AC-02 |
| IAM-05 | Employ the least privilege principle when implementing information system access. | AC-02 |
| IAM-06 | Define and implement a user access provisioning process which authorizes,records, and communicates access changes to data and assets. | AC-03 |
| IAM-07 | De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adapt and communicate identity and access management policies. | AC-06 |
| IAM-08 | Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance. | AC-07 |
| IAM-09 | Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated. | AC-02, AC-09 |
| IAM-10 | Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access. | AC-02 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| IAM-11 | Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles. | IS-03 |
| IAM-12 | Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures. | AC-02 |
| IAM-13 | Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs. | AC-01 |
| IAM-14 | Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets,including multi factor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities. | AC-04, AC-05, CR-01 |
| IAM-15 | Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords. | AC-04 |
| IAM-16 | Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized. | AC-04, AC-05, AC-07 |
| **Interoperability & Portability** | | |
| IPY-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: Communications between application interfaces. Information processing interoperability. Application development portability. Information/Data exchange, usage, portability, integrity, and persistence. Review and update the policies and procedures at least annually. | IS-03, OM-06 |
| IPY-02 | Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability. | CR-01 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| IPY-03 | Implement cryptographically secure and standardized network protocols for the management, import and export of data. | CR-01 |
| IPY-04 | Agreements must include provisions specifying CSCs access to data upon contract termination and will include: Data format. Length of time the data will be stored. Scope of the data retained and made available to the CSCs. Data deletion policy | IS-06, OM-03, OM-04 |
| **Infrastructure & Virtualization Security** | | |
| IVS-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Reviewand update the policies and procedures at least annually. | IS-03 |
| IVS-02 | Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business. | BC-01, BC-02, BC-03, BC-04 |
| IVS-03 | Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls. | OM-01, SC-01, SC-02 |
| IVS-04 | Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls,as part of a security baseline. | AC-08 |
| IVS-05 | Separate production and non-production environments. | CM-03 |
| IVS-06 | Design, develop, deploy and configure applications and infrastructures such that CSC and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants. | This control was not included in the scope of the SOC examination. |
| IVS-07 | Use secure and encrypted communication channels when migrating servers,services, applications, or data to cloud environments. Such channels must includeonly up-to-date and approved protocols. | CR-01 |
| IVS-08 | Identify and document high-risk environments. | RC-1 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| IVS-09 | Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks. | OM-01 |
| **Logging and Monitoring** | | |
| LOG-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually. | OM-01, OM-02 |
| LOG-02 | Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs. | OM-01 |
| LOG-03 | Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics. | OM-01 |
| LOG-04 | Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability. | AC-01, AC-02 |
| LOG-05 | Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies. | OM-01 |
| LOG-06 | Use a reliable time source across all relevant information processing systems. | This control was not included in the scope of the SOC examination. |
| LOG-07 | Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment. | OM-01 |
| LOG-08 | Generate audit records containing relevant security information. | OM-01 |
| LOG-09 | The information system protects audit records from unauthorized access,modification, and deletion. | AC-02 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| LOG-10 | Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls. | OM-01 |
| LOG-11 | Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys. | OM-01 |
| LOG-12 | Monitor and log physical access using an auditable access control system. | IS-03 |
| LOG-13 | Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party. | OM-01, OM-02 |
| **Security Incident Management, E-Discovery, & Cloud Forensics** | | |
| SEF-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and CloudForensics. Review and update the policies and procedures at least annually. | OM-01 |
| SEF-02 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Reviewand update the policies and procedures at least annually. | IS-06, OM-01 |
| SEF-03 | 'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships(such as supply-chain) that may be impacted.' | OM-01 |
| SEF-04 | Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness. | OM-01 |
| SEF-05 | Establish and monitor information security incident metrics. | OM-01, RC-04 |
| SEF-06 | Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events. | OM-01, RC-04 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| SEF-07 | Define and implement processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs,laws and regulations. | IS-06, PR-10 |
| SEF-08 | Maintain points of contact for applicable regulation authorities,national and local law enforcement, and other legal jurisdictional authorities. | OM-01 |
| **Supply Chain Management, Transparency, and Accountability** | | |
| STA-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security ResponsibilityModel (SSRM) within the organization. Review and update the policies and procedures at least annually. | IS-03, RC-02 |
| STA-02 | Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering. | RC-02 |
| STA-03 | Provide SSRM Guidance to the CSC detailing information about theSSRM applicability throughout the supply chain. | RC-02 |
| STA-04 | Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering. | IS-03 |
| STA-05 | Review and validate SSRM documentation for all cloud services offerings the organization uses. | IS-03 |
| STA-06 | Implement, operate, and audit or assess the portions of the SSRMwhich the organization is responsible for. | IS-03 |
| STA-07 | Develop and maintain an inventory of all supply chain relationships. | RC-02 |
| STA-08 | CSPs periodically review risk factors associated with all organizations within their supply chain. | RC-02 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| STA-09 | Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: Scope, characteristics and location of business relationship and services offered. Information security requirements (including SSRM). Change management process. Logging and monitoring capability. Incident management and communication procedures. Right to audit and third party assessment. Service termination. Interoperability and portability requirements. Data privacy. | OM-03 |
| STA-10 | Review supply chain agreements between CSPs and CSCs at least annually. | RC-02 |
| STA-11 | Define and implement a process for conducting internal assessment to confirm conformance and effectiveness of standards, policies, procedures,and service level agreement activities at least annually. | IS-03, RC-02 |
| STA-12 | Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy,audit, personnel policy and service level requirements and standards. | OM-05, RC-02 |
| STA-13 | Periodically review the organization's supply chain partners' ITgovernance policies and procedures. | RC-02 |
| STA-14 | Define and implement a process for conducting security assessments periodically for all organizations within the supply chain. | RC-02 |
| **Threat & Vulnerability Management** | | |
| TVM-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually. | IS-03 |
| TVM-02 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually. | TV-02 |
| TVM-03 | Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications,based on the identified risk. | OM-01 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| TVM-04 | Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis. | OM-01 |
| TVM-05 | Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy. | CM-06, OM-01 |
| TVM-06 | Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties. | TV-01 |
| TVM-07 | Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly. | CM-06 |
| TVM-08 | Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework. | OM-02 |
| TVM-09 | Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification. | CM-06, OM-01 |
| TVM-10 | Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals. | CM-06 |
| **Universal Endpoint Management** | | |
| UEM-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually. | IS-03, TV-02 |
| UEM-02 | Define, document, apply and evaluate a list of approved services,applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data. | IS-03 |
| UEM-03 | Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications. | TV-02 |
| UEM-04 | Maintain an inventory of all endpoints used to store and access company data. | AM-01 |

| CSA CCM Control ID | Control Description | Avaamo Mapping |
|---|---|---|
| UEM-05 | Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data. | IS-03, AM-01 |
| UEM-06 | Configure all relevant interactive-use endpoints to require an automatic lock screen. | This control was not included in the scope of the SOC examination. |
| UEM-07 | Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes. | CM-01, CM-05 |
| UEM-08 | Protect information from unauthorized disclosure on managed endpoint devices with storage encryption. | CR-02, TV-02 |
| UEM-09 | Configure managed endpoints with anti-malware detection and prevention technology and services. | TV-02 |
| UEM-10 | Configure managed endpoints with properly configured software firewalls. | This control was not included in the scope of the SOC examination. |
| UEM-11 | Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment. | This control was not included in the scope of the SOC examination. |
| UEM-12 | Enable remote geo-location capabilities for all managed mobile endpoints. | This control was not included in the scope of the SOC examination. |
| UEM-13 | Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices. | AM-01, TV-02 |
| UEM-14 | Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets. | AC-03, AC-04, AC-07, AM-01 |

# Additional Information Provided by Avaamo to Provide a Mapping of Avaamo Controls to the HITRUST CSF Version 9.4

The HITRUST CSF provides the structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their data protection compliance. The initial development of the HITRUST CSF leveraged nationally and internationally accepted security and privacy-related regulations, standards, and frameworks, including ISO, NIST, PCI, HIPAA, and COBIT, to ensure a comprehensive set of security and privacy controls, and continually incorporates additional authoritative sources.

The table below includes a mapping of the HITRUST CSF version 9.4 to the SOC 2 controls included in this SOC 2 examination.

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 0.0 Information Security Management Program | 00.a Information Security Management Program | An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement. | IS-1, RC-1, RC-2 |
| 01.0 Access Control | 01.b User Registration | There shall be a formal documented and implemented user registration and de-registration procedure for granting and revoking access. | AC-03, AC-06 |
| | 01.c Privilege Management | The allocation and use of privileges to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls. | AC-01, AC-02, AC-03, AC-06, AC-07, AC-09 |
| | 01.d User Password Management | Passwords shall be controlled through a formal management process. | AC-04, AC-05 |
| | 01.e Review of User Access Rights | All access rights shall be regularly reviewed by management via a formal documented process. | AC-07 |

| | | | |
|---|---|---|---|
| | 01.h Clear Desk and Clear Screen Policy | A Clear Desk Policy for papers and removable storage media and a Clear Screen Policy for information assets shall be adopted. | Currently, Avaamo's SOC 2 controls do not directly map to 01.h |
| | 01.j User Authentication for External Connections | Appropriate authentication methods shall be used to control access by remote users. | AC-01, AC-02, AC-03, AC-04, AC-05, AC-08 |
| | 01.l Remote Diagnostic and Configuration Port Protection | Physical and logical access to diagnostic and configuration ports shall be controlled. | AC-08, AM-1, SC-1, SC-2 |
| | 01.m Segregation in Networks | Groups of information services, users, and information systems should be segregated on networks. | AC-02, AC-03, AC-08, AC-09, SC-1, SC-2 |
| | 01.n Network Connection Control | For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the Access Control Policy and requirements of the business applications. | AC-01, AC-04, AC-05, SC-1, SC-2 |
| | 01.o Network Routing Control | Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the Access Control Policy of the business applications. | AC-08, SC-1, SC-2 |
| | 01.q User Identification and Authentication | All users shall have a unique identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user. | AC-01, AC-04, AC-05, AC-08 |
| | 01.t Session Time-out | Inactive sessions shall shut down after a defined period of inactivity. | AC-04 |

| | | | |
|---|---|---|---|
| | 01.v Information Access Restriction | Logical and physical access to information and application systems and functions by users and support personnel shall be restricted in accordance with the defined Access Control Policy. | AC-01, AC-02, AC-04, AC-05 |
| | 01.w Sensitive System Isolation | Sensitive systems shall have a dedicated and isolated computing environment. | AC-02, AC-03, AC-04, AC-05 |
| | 01.x Mobile Computing and Communications | A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication devices. | AC-04, AC-05 |
| | 01.y Teleworking | A policy, operational plans and procedures shall be developed and implemented for teleworking activities. | IS-3 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 02.0 Human Resources Security | 02.a Roles and Responsibilities | Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the organization's Information Security Policy. | HR-2, IS-1, IS-5 |
| | 02.d Management Responsibilities | Management shall require employees, and where applicable, contractors and third-party users, to apply security in accordance with established policies and procedures of the organization. | HR-2, IS-1, IS-5, RC-3 |
| | 02.e Information Security Awareness, Education, and Training | All employees of the organization, and contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. | HR-2, IS-1, IS-2, IS-5 |
| | 02.f Disciplinary Process | There shall be a formal disciplinary process for employees who have violated security policies and procedures. | HR-2, IS-1, OM-02 |
| | 02.i Removal of Access Rights | The access rights of all employees, contractors, and third-party users to information and information assets shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment (i.e. upon transfer within the organization). | AC-06, AC-07 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 03.0 Risk Management | 03.b Performing Risk Assessments | Risk Assessments shall be performed to identify and quantify risks. | RC-1, RC-2, RC-3, TV-1 |
| | 03.c Risk Mitigation | Risks shall be mitigated to an acceptable level. | RC-1, RC-2, RC-3, TV-1 |
| | 03.d Risk Evaluation | Risks shall be continually evaluated and assessed. | CM-5, RC-1, RC-2, RC-3, TV-1 |
| 04.0 Security Policy | 04.a Information Security Policy Document | Information Security Policy documents shall be approved by management, and published and communicated to all employees and relevant external parties. Information Security Policy documents shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security Policy documents shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles. | IS-1, IS-3, IS-5 |
| | 04.b Review of the Information Security Policy | The Information Security Policy documents shall be reviewed at planned intervals or if significant changes occur to ensure its continuing adequacy and effectiveness. | IS-1, IS-3 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 05.0 Organization of Information Security | 05.a Management Commitment to Information Security | Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. | HR-2, IS-1, IS-2, IS-3 |
| | 05.h Independent Review of Information Security | The organization's approach to managing information security and its implementation (control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, at a minimum annually, or when significant changes to the security implementation occur. | RC-1, RC-3, TV-1, TV-2 |
| | 05.i Identification of Risks Related to External Parties | The risks to the organization's information and information assets from business processes involving external parties shall be identified, and appropriate controls implemented before granting access. | RC-2, RC-3 |
| | 05.j Addressing Security When Dealing with Customers | All identified security requirements shall be addressed before giving customers access to the organization's information or assets. | OM-04, RC-1 |
| | 05.k Addressing Security in Third Party Agreements | Agreements with third-parties involving accessing, processing, communicating or managing the organization's information or information assets, or adding products or services to information assets shall cover all relevant security requirements. | RC-1, RC-2 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 06.0 Compliance | 06.c Protection of Organizational Records | Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. | AM-1, CR-1, CR-2, HR-2, OM-06 |
| | 06.d Data Protection and Privacy of Covered Information | Data protection and privacy shall be ensured as required in relevant legislation, regulations, and contractual clauses. | AC-02, AC-03, AC-04, AC-05, AC-06, CR-1, CR-2 |
| | 06.e Prevention of Misuse of Information Assets | Users shall be deterred from using information assets for unauthorized purposes. | HR-2, IS-1, IS-2, IS-3 |
| | 06.g Compliance with Security Policies and Standards | Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. | HR-2, IS-2 |
| | 06.h Technical Compliance Checking | Information systems shall be regularly checked for compliance with security implementation standards. | OM-01, TV-1 |
| 07.0 Asset Management | 07.a Inventory of Assets | All assets including information shall be clearly identified and an inventory of all assets drawn up and maintained. | AM-1 |
| | 07.c Acceptable Use of Assets | Rules for the acceptable use of information and assets associated with information processing systems shall be identified, documented, and implemented. | HR-2, IS-3 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 08.0 Physical and Environmental Security | 08.b Physical Entry Controls | Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | This control is not applicable for Avaamo as they do not have physical access to any media that stores customer information. AWS is responsible for this control. See 'Complementary Subservice Organization Controls' section above. |
| | 08.d Protecting Against External and Environmental Threats | Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. | All servers supporting the Avaamo Conversational AI platform are housed in AWS. See 'Complementary Subservice Organization Controls' section above. |
| | 08.j Equipment Maintenance | Equipment shall be correctly maintained to ensure its continued availability and integrity. | All servers supporting the Avaamo Conversational AI platform are housed in AWS. See 'Complementary Subservice Organization Controls' section above. |
| | 08.l Secure Disposal or Re-Use of Equipment | All items of equipment containing storage media shall be checked to ensure that any covered information and licensed software has been removed or securely overwritten prior to disposal. | AM-1 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 09.0 Communications and Operations Management | 09.b Change Management | Changes to information assets and systems shall be controlled and archived. | CM-1, CM-6 |
| | 09.c Segregation of Duties | Separation of duties shall be enforced to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. | AC-01, AC-03, AC-06, AC-06 |
| | 09.e Service Delivery | It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party. | RC-1, RC-2 |
| | 09.f Monitoring and Review of Third Party Services | The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements. | IS-1, RC-1, RC-2 |
| | 09.j Controls Against Malicious Code | Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided. | AM-1, OM-01, OM-02, RC-3, TV-1, TV-3 |
| | 09.k Controls Against Mobile Code | Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined Security Policy. All unauthorized mobile code shall be prevented from executing. | AC-08, CM-1, CM-3, CM-6, TV-1, TV-3 |
| | 09.l Back-up | Back-up copies of information and software shall be taken and tested regularly. | BC-1, BC-2, BC-3 |

| | | | |
|---|---|---|---|
| | 09.m Network Controls | Networks shall be managed and controlled in order to protect the organization from threats and to maintain security for the systems and applications using the network, including information in transit. | AC-02, AC-04, AC-05, AC-06, SC-1, SC-2 |
| | 09.n Security of Network Services | Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. | AC-01, AC-02, AC-03, SC-1, SC-2 |
| | 09.o Management of Removable Media | Formal procedures shall be documented and implemented for the management of removable media. | HR-2, IS-3 |
| | 09.p Disposal of Media | Media shall be disposed of securely and safely when no longer required, using formal procedures that are documented. | AM-1, TV-3 |
| | 09.q Information Handling Procedures | Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. | IS-3 |
| | 09.s Information Exchange Policies and Procedures | Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication mediums. | AC-08, CR-1, OM-01, SC-1, SC-2, TV-3 |
| | 09.v Electronic Messaging | Information involved in electronic messaging shall be appropriately protected. | CR-1 |
| | 09.x Electronic Commerce Services | Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure or modification. | Electronic Commerce Services are not within the scope of this engagement. |

| | | | |
|---|---|---|---|
| | 09.y On-line Transactions | Information involved in online transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | On-line Transactions are not within the scope of this engagement. |
| | 09.aa Audit Logging | Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. | AM-1, OM-01 |
| | 09.ab Monitoring System Use | Procedures for monitoring use of information processing systems and facilities shall be established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly. | AM-1, OM-01 |
| | 09.ad Administrator and Operator Logs | System administrator and system operator activities shall be logged and regularly reviewed. | OM-01 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 10.0 Information Systems Acquisition, Development, and Maintenance | 10.a Security Requirements Analysis and Specification | Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems shall specify the requirements for security controls. | AC-09, AM-1, CM-6, OM-01, TV-1 |
| | 10.b Input Data Validation | Data input to applications and databases shall be validated to ensure that this data is correct and appropriate. | OM-04, OM-06 |
| | 10.f Policy on the Use of Cryptographic Controls | A policy on the use of cryptographic controls for protection of information shall be developed and implemented, and supported by formal procedures. | CR-1, CR-2, IS-3, IS-5, IS-6 |
| | 10.h Control of Operational Software | There shall be procedures in place to control the installation of software on operational systems. | AC-09, CM-1, CM-4, OM-01, OM-06 |
| | 10.k Change Control Procedures | The implementation of changes, including patches, service packs, and other updates and modifications, shall be controlled by the use of formal change control procedures. | CM-1, CM-4, CM-5, CM-6 |
| | 10.l Outsourced Software Development | Outsourced software development shall be supervised and monitored by the organization. | CM-6, RC-2 |
| | 10.m Control of Technical Vulnerabilities | Timely information about technical vulnerabilities of information systems being used shall be obtained; the organization's exposure to such vulnerabilities evaluated; and appropriate measures taken to address the associated risk. | OM-01, RC-1, RC-3, TV-1, TV-2 |

| HITRUST CSF Control Category Name | HITRUST Control Reference | HITRUST Control Description | Supporting Avaamo Control |
|---|---|---|---|
| 11.0 Information Security Incident | 11.a Reporting Information Security Events | Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third-party users shall be made aware of their responsibility to report any information security events as quickly as possible. | BC-1, OM-01, OM-02, OM-04, RC-2, TV-1, TV-2 |
| | 11.c Responsibilities and Procedures | Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. | BC-1, IS-1, OM-01, OM-02, OM-04, RC-2, TV-1, TV-2 |
| | 11.d Learning from Information Security Incidents | There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. | BC-1, OM-01, OM-02, RC-2, TV-1, TV-2 |
| 12.0 Business Continuity Management | 12.b Business Continuity and Risk Assessment | Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security. | BC-1, BC-2, BC-3, RC-1, RC-2 |
| | 12.c Developing and Implementing Continuity Plans Including Information Security | Plans shall be developed and implemented to maintain or restore operations and ensure availability of information, at the required level and in the required time scales, following interruption to, or failure of, critical business processes. | BC-1, BC-2 |
| | 12.d Business Continuity Planning Framework | A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. | BC-1, BC-2 |

# Additional Information Provided by Avaamo to Provide a Mapping of ISO/IEC 27001:2022

ISO/IEC 27001 formally specifies an information security management system (ISMS), a governance arrangement comprising a structured suite of activities with which to manage information risks. The ISMS is an overarching framework through which management identifies, evaluates, and treats (addresses) the organization's information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities, and business impacts.

The table below includes a mapping of the ISO/IEC 27001:2022 Annex A to the SOC 2 controls included in this SOC 2 examination.

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| **A.5 – Organizational Controls** | | |
| A.5.01 | IS-01, IS-02, IS-04, HR-01 | An Information Security Policy and topic-specific policies shall be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. |
| A.5.02 | IS-01, IS-02, IS-04 | Information security roles and responsibilities shall be defined and allocated according to the organization needs. |
| A.5.03 | IS-01, AC-09 | Conflicting duties and conflicting areas of responsibility shall be segregated. |
| A.5.04 | HR-01, IS-01, IS-02, IS-03, IS-06 | Management shall require all personnel to apply information security in accordance with the established Information Security Policy, topic-specific policies and procedures of the organization. |
| A.5.05 | RC-01, RC-02, IS-06, IS-07, IS-08 | The organization shall establish and maintain contact with relevant authorities. |
| A.5.06 | IS-01, IS-07, RC-01, RC-02 | The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations. |
| A.5.07 | OM-01, OM-02, OM-04, RC-01, RC-06 | Information relating to information security threats shall be collected and analyzed to produce threat intelligence. |
| A.5.08 | IS-04, AC-08, CM-01, CM-04 | Information security shall be integrated into project management. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.5.09 | AM-01, RC-01, TV-03 | An inventory of information and other associated assets, including owners, shall be developed and maintained. |
| A.5.10 | HR-01, IS-04, OM-03, RC-01 | Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented, and implemented. |
| A.5.11 | AC-06, AM-01 | Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement. |
| A.5.12 | OM-03, RC-01 | Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements. |
| A.5.13 | AM-01, IS-04, OM-03, RC-01, OM-04 | An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |
| A.5.14 | AC-02, AC-03, AC-07, AC-08, CR-01, SC-01, SC-02, RC-04 | Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties. |
| A.5.15 | IS-04, AC-01, AC-02, AC-03, SC-01 | Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. |
| A.5.16 | AC-01, AC-02, AC-03, AC-06, AC-07 | The full life cycle of identities shall be managed. |
| A.5.17 | AC-02, AC-04, AC-05, HR-01, IS-04 | Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. |
| A.5.18 | AC-04, AC-06, AC-07 | Access rights to information and other associated assets shall be provisioned, reviewed, modified, and removed in accordance with the organization's topic-specific policy on and rules for access control. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.5.19 | RC-03, RC-04 | Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. |
| A.5.20 | RC-03, RC-04 | Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. |
| A.5.21 | RC-03, RC-04 | Processes and procedures shall be defined and implemented to manage the information security risks associated with the information and communication technology (ICT) products and services supply chain. |
| A.5.22 | RC-01, RC-02, RC-03, RC-04 | The organization shall regularly monitor, review, evaluate, and manage change in supplier information security practices and service delivery. |
| A.5.23 | RC-03, RC-04 | Processes for acquisition, use, management, and exit from cloud services shall be established in accordance with the organization's information security requirements. |
| A.5.24 | OM-01, OM-02 | The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities. |
| A.5.25 | OM-01, OM-02, TV-01 | The organization shall assess information security events and decide if they are to be categorized as information security incidents. |
| A.5.26 | OM-01, OM-02 | Information security incidents shall be responded to in accordance with the documented procedures. |
| A.5.27 | OM-01, OM-02, RC-01 | Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. |
| A.5.28 | OM-01, OM-02 | The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events. |
| A.5.29 | BC-01, BC-02, BC-03, IS-04, RC-01 | The organization shall plan how to maintain information security at an appropriate level during disruption. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.5.30 | BC-01 | ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. |
| A.5.31 | CR-01, CR-02, IS-04, RC-01 | Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented, and kept up to date. |
| A.5.32 | HR-01, IS-04, O M-03, RC-01 | The organization shall implement appropriate procedures to protect intellectual property rights. |
| A.5.33 | BC-02, BC-03, AC-02, CR-02 | Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release. |
| A.5.34 | CR-02, HR-01, OM-03, RC-01 | The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. |
| A.5.35 | RC-01, RC-02, RC-05 | The organization's approach to managing information security and its implementation including people, processes, and technologies shall be reviewed independently at planned intervals, or when significant changes occur. |
| A.5.36 | IS-04, RC-01, RC-03, RC-05 | Compliance with the organization’s Information Security Policy, topic-specific policies, rules, and standards shall be regularly reviewed. |
| A.5.37 | IS-04, IS-06, IS-07 | Operating procedures for information processing facilities shall be documented and made available to personnel who need them. |
| **A.6 - People Controls** | | |
| A.6.01 | HR-03 | Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. |
| A.6.02 | HR-01 | The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.6.03 | HR-01, IS-03 | Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training, and regular updates of the organization's Information Security Policy, topic-specific policies and procedures, as relevant for their job function. |
| A.6.04 | HR-01, IS-04 | A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an Information Security Policy violation. |
| A.6.05 | AC-06, AC-07, HR-01 | Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced, and communicated to relevant personnel and other interested parties. |
| A.6.06 | HR-01, OM-03, RC-04 | Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties. |
| A.6.07 | IS-04 | Security measures shall be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organization's premises. |
| A.6.08 | IS-08, OM-01, OM-02, TV-01, TV-02, IS-07 | The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. |
| **A.7 – Physical Controls** | | |
| A.7.01 | See Complementary Subservice Organization Controls section within the report. | Security perimeters shall be defined and used to protect areas that contain information and other associated assets. |
| A.7.02 | See Complementary Subservice Organization Controls section within the report. | Secure areas shall be protected by appropriate entry controls and access points. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.7.03 | See Complementary Subservice Organization Controls section within the report. | Physical security for offices, rooms, and facilities shall be designed and implemented. |
| A.7.04 | See Complementary Subservice Organization Controls section within the report. | Premises shall be continuously monitored for unauthorized physical access. |
| A.7.05 | See Complementary Subservice Organization Controls section within the report. | Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. |
| A.7.06 | See Complementary Subservice Organization Controls section within the report. | Security measures for working in secure areas shall be designed and implemented. |
| A.7.07 | See Complementary Subservice Organization Controls section within the report. | Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. |
| A.7.08 | See Complementary Subservice Organization Controls section within the report. | Equipment shall be sited securely and protected. |
| A.7.09 | AM-01, TV-03 | Off-site assets shall be protected. |
| A.7.10 | IS-04, TV-03, AM-01, OM-03 | Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements. |
| A.7.11 | See Complementary Subservice Organization Controls section within the report. | Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.7.12 | See Complementary Subservice Organization Controls section within the report. | Cables carrying power, data, or supporting information services shall be protected from interception, interference, or damage. |
| A.7.13 | AM-01, TV-03 | Equipment shall be maintained correctly to ensure availability, integrity, and confidentiality of information. |
| A.7.14 | AM-01, TV-03 | Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |
| **A.8 – Technological Controls** | | |
| A.8.01 | IS-04, TV-03 | Information stored on, processed by or accessible via user end point devices shall be protected. |
| A.8.02 | AC-02, AC-04, AC-05, AC-07, AC-09 | The allocation and use of privileged access rights shall be restricted and managed. |
| A.8.03 | AC-02, AC-04, AC-05, AC-07, AC-09 | Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. |
| A.8.04 | AC-02, AC-09 | Read and write access to source code, development tools, and software libraries shall be appropriately managed. |
| A.8.05 | AC-01, AC-04, AC-05 | Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. |
| A.8.06 | BC-01, BC-04, OM-01 | The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. |
| A.8.07 | HR-01, IS-03, OM-01, TV-01, TV-02, TV-03 | Protection against malware shall be implemented and supported by appropriate user awareness. |
| A.8.08 | OM-01, RC-01, RC-02, RC-03, RC-04, TV-01, TV-02, IS-04 | Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.8.09 | AC-08, OM-01, RC-05 | Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored, and reviewed. |
| A.8.10 | OM-03, TV-03 | Information stored in information systems, devices, or any other storage media shall be deleted when no longer required. |
| A.8.11 | N/A - No SOC mapping to this ISO Control | Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. |
| A.8.12 | N/A - No SOC mapping to this ISO Control | Data leakage prevention measures shall be applied to systems, networks, and any other devices that process, store, or transmit sensitive information. |
| A.8.13 | BC-01, BC-03 | Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. |
| A.8.14 | BC-01, BC-02, BC-03 | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. |
| A.8.15 | AC-02, AC-08, BC-02, OM-01, OM-04, RC-01, RC-05, SC-01, SC-02, TV-01 | Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected, and analyzed. |
| A.8.16 | AC-02, AC-08, BC-02, OM-01, RC-01, RC-05, SC-01, SC-02, TV-01 | Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents. |
| A.8.17 | AC-08 | The clocks of information processing systems used by the organization shall be synchronized to approved time sources. |
| A.8.18 | AC-02, AC-09 | The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled. |
| A.8.19 | AC-08, CM-01, CM-02, CM-04, IS-07, TV-03 | Procedures and measures shall be implemented to securely manage software installation on operational systems. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.8.20 | AC-02, AC-05, AC-07, CR-01, SC-01, SC-02 | Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. |
| A.8.21 | CR-01, SC-01, SC-02, RC-04 | Security mechanisms, service levels and service requirements of network services shall be identified, implemented, and monitored. |
| A.8.22 | AC-02, AC-04, AC-05, AC-08, SC-01, SC-02 | Groups of information services, users, and information systems shall be segregated in the organization's networks. |
| A.8.23 | N/A - No SOC mapping to this ISO Control | Access to external websites shall be managed to reduce exposure to malicious content. |
| A.8.24 | CR-01, CR-02, IS-04 | Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. |
| A.8.25 | AC-08, CM-01, CM-02, IS-06 | Rules for the secure development of software and systems shall be established and applied. |
| A.8.26 | AC-08, CM-01, CM-02, CM-04, CR-01, OM-01, SC-01 | Information security requirements shall be identified, specified, and approved when developing or acquiring applications. |
| A.8.27 | AC-08, CM-01, CM-02, CM-03, CM-04, CM-05, IS-03, IS-06 | Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities. |
| A.8.28 | CM-01, CM-02, CM-03, CM-05 | Secure coding principles shall be applied to software development. |
| A.8.29 | CM-01, CM-02, CM-03, CM-04, CM-05 | Security testing processes shall be defined and implemented in the development life cycle. |
| A.8.30 | N/A - does not outsource development. | The organization shall direct, monitor, and review the activities related to outsourced system development. |
| A.8.31 | AC-02, CM-03 | Development, testing and production environments shall be separated and secured. |

| ISO 27001:2022 Control ID | Supporting Avaamo Control | ISO Control Description |
|---|---|---|
| A.8.32 | CM-01, CM-02, CM-03, CM-04, CM-05, AC-07, AC-08, AC-09 | Changes to information processing facilities and information systems shall be subject to change management procedures. |
| A.8.33 | CM-01, CM-02, CM-03 | Test information shall be appropriately selected, protected, and managed. |
| A.8.34 | AC-07, AC-09, BC-01, BC-04, IS-02, RC-02, TV-01, TV-02 | Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. |

# Additional Information Provided by Avaamo to Provide a Mapping to NIST 800-171 Security Revision 2 Requirements

Published in February 2020 and revised January 28, 2021, NIST 800-171 Revision 2 special publication provides agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CU)I when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and non-federal organizations.

The table below includes a mapping of the NIST 800-171 to the SOC 2 controls included in this SOC 2 examination.

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| **3.1 Access Control** | | |
| 3.1.1 | AC-01, AC-02 AC-03, AC-04, AC-08, AC-05, AC-06, CR-01, CR-02, SC-01, IS-03, OM-01 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). |
| 3.1.2 | AC-01, AC-02, AC-03, AC-05, HR-02, IS-03, OM-01,SC-01, TV-03 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. |
| 3.1.3 | AC-01, AC-05, SC-01, CR-01, CR-02, TV-03 | Control the flow of CUI in accordance with approved authorizations. |
| 3.1.4 | AC-03, AC-05, AC-06, AC-08 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. |
| 3.1.5 | AC-01, AC-02, AC-03, AC-05, AC-06, AC-08 | Employ the principle of least privilege, including for specific security functions and privileged accounts. |
| 3.1.6 | AC-01, AC-02, AC-03, AC-05, AC-06 AC-08 | Use non-privileged accounts or roles when accessing non-security functions. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.1.7 | AC-01, AC-02, AC-05, AC-06, TV-01, TV-02, TV-03 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. |
| 3.1.8 | AC-04 | Limit unsuccessful logon attempts. |
| 3.1.9 | IS-01, IS-02, IS-03, OM-05 | Provide privacy and security notices consistent with applicable CUI rules. |
| 3.1.10 | AC-04, AC-05 | Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. |
| 3.1.11 | AC-04 | Terminate (automatically) a user session after a defined condition. |
| 3.1.12 | AC-05, AC-02, OM-01 | Monitor and control remote access sessions. |
| 3.1.13 | AC-05, CR-01, CR-02 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. |
| 3.1.14 | AC-01, AC-05 | Route remote access via managed access control points. |
| 3.1.15 | AC-01, AC-05, AC-02 | Authorize remote execution of privileged commands and remote access to security relevant information. |
| 3.1.16 | N/A - The wireless network at the corporate office is physically and logically separated from the corporate networks hosted in the data centers. The wireless network at the office is used to connect only to the internet, the password is only known by Avaamo employees, and it does not allow access to any Avaamo production infrastructure or other key systems. | Authorize wireless access prior to allowing such connections. |
| 3.1.17 | | Protect wireless access using authentication and encryption. |
| 3.1.18 | AC-05, SC-01 | Control connection of mobile devices. |
| 3.1.19 | CR-01, CR-02 | Encrypt controlled unclassified information (CUI) on mobile devices and mobile computing platforms. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.1.20 | AC-01, SC-01, OM-01, TV-03 | Verify and control/limit connections to and use of external systems. |
| 3.1.21 | IS-03 | Limit use of portable storage devices on external systems. |
| 3.1.22 | HR-02, IS-03, IS-06 | Control CUI posted or processed on publicly accessible systems. |
| **3.2 Awareness and Training** | | |
| 3.2.1 | IS-01, IS-02, IS-06, IS-07, IS-05 | Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. |
| 3.2.2 | HR-01, IS-04 | Ensure that personnel are trained to carry out their assigned information security related duties and responsibilities. |
| 3.2.3 | IS-01, IS-02, IS-05 | Provide security awareness training on recognizing and reporting potential indicators of insider threat. |
| **3.3 Audit and Accountability** | | |
| 3.3.1 | AC-08, OM-05, OM-01 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. |
| 3.3.2 | AC-01, AC-08 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. |
| 3.3.3 | OM-04, OM-01, RC-01, TV-01, TV-03 | Review and update logged events. |
| 3.3.4 | OM-04, OM-01, RC-01, TV-03 | Alert in the event of an audit logging process failure. |
| 3.3.5 | OM-04, OM-01, TV-01, TV-02, TV-03 | Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. |
| 3.3.6 | OM-01, TV-03 | Provide audit record reduction and report generation to support on-demand analysis and reporting. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.3.7 | OM-08 | Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. |
| 3.3.8 | AC-08, AC-02, SC-01 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. |
| 3.3.9 | AC-02 | Limit management of audit logging functionality to a subset of privileged users. |
| **3.4 Configuration Management** | | |
| 3.4.1 | AC-08, AM-01 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. |
| 3.4.2 | AC-08, CM-03 | Establish and enforce security configuration settings for information technology products employed in organizational systems. |
| 3.4.3 | CM-07 | Track, review, approve or disapprove, and log changes to organizational systems. |
| 3.4.4 | CM-01, CM-03, CM-07, CM-04 | Analyze the security impact of changes prior to implementation. |
| 3.4.5 | AC-02, CM-01, AC-08 | Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. |
| 3.4.6 | AC-01, AC-02, SC-01 | Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. |
| 3.4.7 | AC-08, SC-01 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. |
| 3.4.8 | AC-08, SC-01 | Apply the Deny-by-exception (Blacklisting) Policy to prevent the use of unauthorized software or deny-all, and the Permit-by-exception (Whitelisting) Policy to allow the execution of authorized software. |
| 3.4.9 | OM-01, OM-02, OM-08 | Control and monitor user-installed software. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| **3.5 Identification and Authentication** | | |
| 3.5.1 | AC-03, AC-04, AC-01, AC-05, CR-01 | Identify system users, processes acting on behalf of users, and devices. |
| 3.5.2 | AC-01, AC-05 | Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. |
| 3.5.3 | AC-05 | Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. |
| 3.5.4 | AC-03, CR-01 | Employ replay resistant authentication mechanisms for network access to privileged and non-privileged accounts. |
| 3.5.5 | AC-01, AC-03 | Prevent reuse of identifiers for a defined period. |
| 3.5.6 | AC-03, AC-06 | Disable identifiers after a defined period of inactivity. |
| 3.5.7 | AC-04 | Enforce a minimum password complexity and change of characters when new passwords are created. |
| 3.5.8 | AC-04 | Prohibit password reuse for a specified number of generations. |
| 3.5.9 | AC-01 | Allow temporary password use for system logons with an immediate change to a permanent password. |
| 3.5.10 | AC-04 | Store and transmit only cryptographically protected passwords. |
| 3.5.11 | CR-01 | Obscure feedback of authentication information. |
| **3.6 Incident Response** | | |
| 3.6.1 | OM-04, OM-01, TV-01, TV-03 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. |
| 3.6.2 | OM-04, OM-01 | Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. |
| 3.6.3 | BC-02 | Test the organizational incident response capability. |
| **3.7 Maintenance** | | |
| 3.7.1 | CM-01, CM-03 | Perform maintenance on organizational systems. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.7.2 | CM-01, CM-03, CM-02, AC-08, CM-03, CM-07, CM-04, CM-05 | Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. |
| 3.7.3 | RC-03 | Ensure equipment removed for off-site maintenance is sanitized of any CUI. |
| 3.7.4 | RC-03 | Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. |
| 3.7.5 | AC-04 | Require multi-factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. |
| 3.7.6 | CM-01, AC-08, CM-04, CM-07, CM-05 | Supervise the maintenance activities of maintenance personnel without required access authorization. |
| **3.8 Media Protection** | | |
| 3.8.1 | N/A - physical protections are the responsibility of the colocation hosting provider. | Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. |
| 3.8.2 | AC-02, AC-03, AC-05, IS-03 | Limit access to CUI on system media to authorized users. |
| 3.8.3 | OM-05 | Sanitize or destroy system media containing CUI before disposal or release for reuse. |
| 3.8.4 | OM-05 | Mark media with necessary CUI markings and distribution limitations. |
| 3.8.5 | RC-03 | Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. |
| 3.8.6 | CR-01, CR-02 | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. |
| 3.8.7 | IS-03, OM-05 | Control the use of removable media on system components. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.8.8 | IS-03, OM-05 | Prohibit the use of portable storage devices when such devices have no identifiable owner. |
| 3.8.9 | N/A - physical protections are the responsibility of the colocation hosting provider. | Protect the confidentiality of backup CUI at storage locations. |
| **3.9 Personnel Security** | | |
| 3.9.1 | HR-01 | Screen individuals prior to authorizing access to organizational systems containing CUI. |
| 3.9.2 | AC-03 | Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. |
| **3.10 Physical Protection** | | |
| 3.10.1 | N/A - physical protections are the responsibility of the colocation hosting provider. | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. |
| 3.10.2 | N/A - physical protections are the responsibility of the colocation hosting provider. | Protect and monitor the physical facility and support infrastructure for organizational systems. |
| 3.10.3 | N/A - physical protections are the responsibility of the colocation hosting provider. | Escort visitors and monitor visitor activity. |
| 3.10.4 | N/A - physical protections are the responsibility of the colocation hosting provider. | Maintain audit logs of physical access. |
| 3.10.5 | N/A - physical protections are the responsibility of the colocation hosting provider. | Control and manage physical access devices. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.10.6 | AC-05, IS-07, RC-03, SC-01, TV-03 | Enforce safeguarding measures for CUI at alternate work sites. |
| **3.11 Risk Assessment** | | |
| 3.11.1 | RC-01 | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. |
| 3.11.2 | TV-01 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. |
| 3.11.3 | TV-01 | Remediate vulnerabilities in accordance with risk assessments. |
| **3.12 Security Assessment** | | |
| 3.12.1 | IS-01, RC-01, RC-03 | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. |
| 3.12.2 | RC-01, TV-01, TV-02 | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. |
| 3.12.3 | RC-01, RC-03 | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. |
| 3.12.4 | AC-08, IS-05 | Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. |
| **3.13 Systems and Communication Protection** | | |
| 3.13.1 | AC-04, AC-05, AC-08, CM-03, CR-01, CR-02, SC-01, TV-03 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. |
| 3.13.2 | SC-01, CM-01 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| 3.13.3 | AC-05 | Separate user functionality from system management functionality. |
| 3.13.4 | AC-08, SC-01, TV-03 | Prevent unauthorized and unintended information transfer via shared system resources. |
| 3.13.5 | SC-01, CR-01 | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. |
| 3.13.6 | SC-01, TV-03 | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). |
| 3.13.7 | AC-08, SC-01 | Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). |
| 3.13.8 | AC-05, CR-01 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. |
| 3.13.9 | AC-04 | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. |
| 3.13.10 | CR-01, CR-02 | Establish and manage cryptographic keys for cryptography employed in organizational systems. |
| 3.13.11 | CR-01, CR-02 | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. |
| 3.13.12 | AC-01, AC-04, AC-05 | Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. |
| 3.13.13 | CM-03 | Control and monitor the use of mobile code. |
| 3.13.14 | N/A - Avaamo does not utilize Voice over Internet Protocol (VoIP) technologies. | Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. |
| 3.13.15 | CR-01, CR-02 | Protect the authenticity of communications sessions. |
| 3.13.16 | CR-02 | Protect the confidentiality of CUI at rest. |

| Criteria | Supporting Avaamo Control | Safeguard Description |
|---|---|---|
| **3.14 System and Information Integrity** | | |
| 3.14.1 | OM-01 OM-04, OM-05, TV-01, TV-02, TV-03 | Identify, report, and correct system flaws in a timely manner. |
| 3.14.2 | TV-01, TV-03 | Provide protection from malicious code at designated locations within organizational systems. |
| 3.14.3 | OM-01, TV-03 | Monitor system security alerts and advisories and take action in response. |
| 3.14.4 | CM-03, TV-01 | Update malicious code protection mechanisms when new releases are available. |
| 3.14.5 | TV-01 | Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed. |
| 3.14.6 | OM-01, TV-03 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. |
| 3.14.7 | OM-01, TV-03 | Identify unauthorized use of organizational systems. |