avaamo

Avaamo, Inc.

Report on Controls at a Service Organization Relevant to Security, Confidentiality, and Availability

SOC 3^{SM} Report

For the Period February 1, 2019 through May 31, 2019

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

BARR
ADVISORY

Independent Service Auditor's Report

To the Management of Avaamo, Inc. (Avaamo):

We have examined management's assertion that Avaamo, during the period of February 1, 2019 through May 31, 2019, maintained effective controls to provide reasonable assurance that:

- the Avaamo Conversational AI system was protected against unauthorized access, use, or modification to meet Avaamo's commitments and system requirements

- the Avaamo Conversational AI system was available for operation and use to meet Avaamo's commitments and system requirements

- the Avaamo Conversational AI system information designated as confidential was protected to meet the entity's commitments and system requirements

based on the criteria for security, confidentiality, and availability in the American Institute of Certified Public Accountants' (AICPA) TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). This assertion is the responsibility of Avaamo management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of Avaamo's relevant controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions based on our findings to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

In our opinion, Avaamo's management assertion referred to below is fairly stated, in all material aspects, based on the aforementioned criteria for security, confidentiality, and availability.

BARR Advisory, P.A.

Fairway, KS
June 17, 2019

Avaamo's Assertion on the Description of the Avaamo Conversational AI System

Avaamo maintained effective controls over the security, confidentiality, and availability of its Avaamo Conversational AI system to provide reasonable assurance that:

- the Avaamo Conversational AI system was protected against unauthorized access, use, or modification to meet Avaamo's commitments and system requirements

- the Avaamo Conversational AI system was available for operation and use to meet Avaamo's commitments and system requirements

- the Avaamo Conversational AI system information designated as confidential was protected to meet the entity's commitments and system requirements

during the period February 1, 2019 through May 31, 2019, based on the criteria for security, confidentiality, and availability principles set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Our attached system description of the Avaamo Conversational AI system identified the aspects of the system covered by our assertion.

Subservice providers are used to perform data center, infrastructure, software, and managed hosting services.

Avaamo, Inc.
June 17, 2019

Overview of Operations

Company Background

Avaamo Service Organization (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 conversational AI platform to the enterprise customers across the globe.

Description of Services Provided

Avaamo's core application, Avaamo Conversational AI application (Avaamo application), is a Software as a Service (SaaS) solution. It is a multi-tenant, multi-user application suite 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 (VA) to corporate employees and their customers.

Avaamo has pioneered 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, Avaamo 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 Conversational AI system include: *Machine Learning, Conversational Design, Continuous Bot Improvement, Vertical Specialization, Enterprise Services, and Voice.*

Machine Learning*: A key part of the Avaamo application, 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 application's machine learning is based on the following technologies:

- *Vertical domains:* Avaamo comes with over 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 web sites and instantly enable virtual assistants to learn and respond using that knowledge.

- *Interaction Engine*: Transcripts, services tickets, 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 are directing users towards 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, language, 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 APIs, Web Services, Enterprise Service Buses (ESB), Message Queues (MQ), Custom Adapters, and much 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 application includes enterprise-wide security, including military grade encryption for data in transit and data at rest, access controls and entitlements, and multi-factor authentication to protect and secure data within the application.

- *Flexible deployment:* Avaamo includes options, based on each entity's environment, for a global 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.
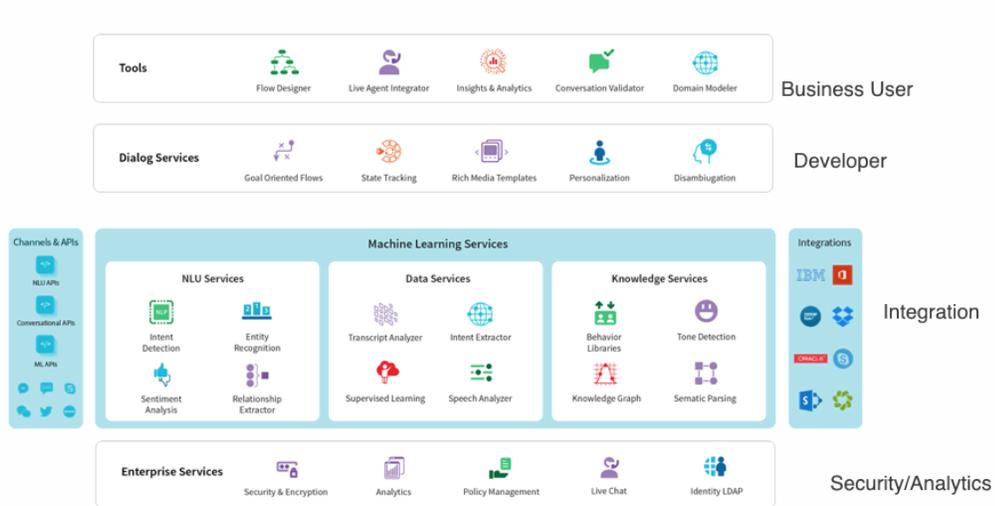
There are three methods and types of users that interact with the Avaamo application. Each method includes different abilities and services, which are summarized below:

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. Customer data includes the user-agent transaction;

   - Update/manage domain models;

   - Create and manage bots;

   - Create and manage knowledge from documents, PDF, raw data uploads, and website, 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;

   - Facebook Messenger;

- Facebook Workplace;

- 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 Conversational AI system 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 Conversational AI system services, and the financial, operational, and compliance requirements that Avaamo has established for the services.

Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Avaamo Conversational AI system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

- 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 application and supporting infrastructure components.

- Use of boundary protection systems, including web application firewalls (WAF), firewalls, and intrusion detection systems.

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.

- Confidentiality and nondisclosure 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 application, including uptime reporting via status.avaamo.com.

- Responses to customer-reported issues within 24 business hours.

Such 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 Conversational AI system.

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 Conversational AI application 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 Conversational AI application are provided by Amazon Web Services (AWS).

Avaamo is responsible for managing the development and operation of the Avaamo application including development and maintenance and infrastructure components such as servers, database and storage systems.

People

Avaamo has a staff of approximately 60 employees 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.

- *Operations*. Manages the deployment, configuration, and monitoring of the Avaamo Conversational AI application.

- *Engineering.* Develop and support the development lifecycle management activities, including software design, coding, quality assurance, security testing 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 focus on demoing and selling the Avaamo Conversational AI system.

Data

Data processed, stored, and transmitted by the Avaamo Conversational AI application is managed by both Avaamo and customer enterprises. The bot developers access the dashboard via 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 ERP, 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 Conversational AI application.

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

- Admin Logins

- Bot definition metadata, which includes the domains, and knowledgebase

- Bot runtime data, which includes the messages the bot exchanged with users

- Bot Insights

- Bot Analytics data

- System files

- Error logs

Data Classification

Data within the Avaamo Conversational AI system 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. Information assets, including customer data, are assigned a classification level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or Company policy, then that classification takes precedence. The classification level then guides the selection of protective measures to secure the information. All data are assigned to one of the following classifications:

- **Customer Classified**: Avaamo shall monitor client data classification level in accordance with client contractual terms or commitments. The client data in this case is the every interaction users have with the bot and the bot responses, including the responses generated from the backend systems 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.'

- **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 nondisclosure agreement, and have a "need to know." This

could include information regarding customers, personnel, payroll, 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; would result in serious personal or financial exposure if revealed to unauthorized persons. This could include strategic planning information prior to general or public disclosure, passwords or any form of security key, etc.

- **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. This includes marketing brochures, published annual reports, press releases, etc.

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. All teams are expected to adhere to Avaamo policies and procedures that define how services should be delivered. These are located on the Company's shared drive and can be accessed by any Avaamo team member.

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;
- Change Management;
- Endpoint Protection;
- Risk Management;
- Third Party Risk Management; and,
- Business Continuity and Disaster Recovery.

Achieving High Security

The Avaamo Conversational AI web application is only accessible over 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 are 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.

Achieving Scalability

Scalability is of critical importance to Avaamo. Avaamo follows service-oriented concepts that provide decoupled, modular services. Operating within a cloud infrastructure, such as AWS, allows Avaamo to scale these services on the fly, both horizontally and vertically. Specifically, AWS load balancers allow Avaamo to scale the system tier up and down as traffic demands.

Achieving High Performance

For the Avaamo Conversational AI web interface, Avaamo ensures responsive page load times by keeping the code algorithmically efficient, reducing the number of layers and using caching where applicable. At the database layer, high performance is achieved through a data model designed with appropriate indexes to facilitate access patterns. Additionally, performance monitoring tools are in place to identify and notify Avaamo of issues related to performance.

Achieving High Availability

High availability is one of the most important architectural considerations at Avaamo. In order to help ensure high availability of Avaamo services, Avaamo ensures all services are able to be deployed or are live across multiple AWS availability zones (multi-AZ). AWS provides services that support multi-AZ automatically, such as, Relational Database Service (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.

Monitoring Performance, Scalability, and Availability

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

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 system is used to provide the service during the period from February 1, 2019 to May 31, 2019.

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 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 application, 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 application periodically to validate appropriateness of access levels.

- User entity is responsible for approving and creating new user access to the Avaamo application.

- User entity is responsible for removing terminated employee access to the Avaamo application.

- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Avaamo application 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 system.

- 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.

- User entity is responsible for communicating to Avaamo specific confidentiality and privacy configurations and commitments including data retention, disposal, and privacy handling.

Complementary Subservice Organization Controls

Avaamo uses subservice organizations for data center, infrastructure, software, and managed hosting services in support of its Avaamo Conversational AI system. Avaamo's controls related to the Avaamo system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria requirements over the Avaamo Conversational AI system 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 organization 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; and,
- Nondisclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Trust Services Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Amazon Web Services	CC6.1
Physical access to the data center facility is restricted to authorized personnel.	Amazon Web Services	CC6.4
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	Amazon Web Services	CC6.4 A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	Amazon Web Services	A1.3