System and Organization Controls (SOC) 2 Type II

Report on Management's Description of

The Eva Platform

Report on Controls Placed in Operation and Test of Operating Effectiveness Relevant to the Trust Services Criteria for Security Category

For the Period
December 10, 2021 to March 10, 2022

Together with
Independent Service Auditor's Report

Table of Contents

I. Independent Service Auditor's Report 1

II. Assertion of EvaBot Inc. Management 5

III. Description of The Eva Platform 6

IV. Description of Test of Controls and Results Thereof 18

I. Independent Service Auditor's Report

Independent Service Auditor's Report

EvaBot Inc.

Scope

We have examined EvaBot Inc.'s accompanying description of its The Eva Platform (system) titled "Description of The Eva Platform" throughout the period December 10, 2021 to March 10, 2022 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria),* (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 10, 2021 to March 10, 2022, to provide reasonable assurance that EvaBot Inc.'s service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

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

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

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

Service Auditor's Responsibilities

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

An examination of the description of a service organization's system and the suitability of the design 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.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual 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 Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a. The description presents EvaBot Inc.'s The Eva Platform (system) that was designed and implemented throughout the period December 10, 2021 to March 10, 2022 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 10, 2021 to March 10, 2022, to provide reasonable assurance that EvaBot Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of EvaBot Inc.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period December 10, 2021 to March 10, 2022, to provide reasonable assurance that EvaBot Inc.'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 EvaBot Inc.'s controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in the section of our report titled "Description of Test of Controls and Results Thereof" is intended solely for the information and use of EvaBot Inc.; user entities of EvaBot Inc.'s The Eva Platform during some or all of the period December 10, 2021 to March 10, 2022, business partners of EvaBot Inc. subject to risks arising from interactions with the EvaBot Inc.'s processing system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

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

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

JohansonGroup LLP

Colorado Springs, Colorado
April 1, 2022

II. Assertion of EvaBot Inc. Management

Assertion of EvaBot Inc. Management

We have prepared the accompanying description of EvaBot Inc.'s "Description of The Eva Platform" for the period December 10, 2021 to March 10, 2022, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria).* The description is intended to provide report users with information about the EvaBot Inc.'s The Eva Platform (system) that may be useful when assessing the risks arising from interactions with EvaBot Inc.'s system, particularly information about system controls that EvaBot Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA, Trust Services Criteria).*

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

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

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

a. The description presents EvaBot Inc.'s The Eva Platform (system) that was designed and implemented throughout the period December 10, 2021 to March 10, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 10, 2021 to March 10, 2022, to provide reasonable assurance that EvaBot Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of EvaBot Inc.'s controls throughout that period.
c. The controls stated in the description operated effectively throughout the period December 10, 2021 to March 10, 2022, to provide reasonable assurance that EvaBot Inc.'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 EvaBot Inc.'s controls operated effectively throughout that period.

EvaBot Inc. Management
April 1, 2022

III. Description of The Eva Platform

Description of The Eva Platform

COMPANY BACKGROUND

EvaBot Company (Rabi Gupta) was founded in Delaware in March 2016 and has employees based throughout the US.

EvaBot is a one-stop shop to automate corporate gift-giving while collecting hyper-personal data and delivering measurable ROI (like testimonials, surveys, meetings) using an AI conversational bot.

EvaBot was founded by a group of veteran entrepreneurs from iDubba and Star TV with deep experience in data integration and simple, intuitive user experience, and is backed by Bloomberg Beta, Precursor Ventures, and a cadre of top-tier angel investors.

SERVICES PROVIDED

The EvaBot application makes it incredibly easy for businesses to automate corporate gift-giving using data and AI.

EvaBot also provides tools for building corporate relationships.

EvaBot is designed to be secure by default, with a novel architecture that offloads as much synchronization logic as possible to the customer's own data warehouse and allows EvaBot to sync megabytes of data quickly without storing that data in our systems.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

EvaBot designs its processes and procedures related to its platform to meet its objectives for gifting automation services. Those objectives are based on the service commitments that EvaBot makes to user entities, the laws and regulations that govern the provision of EvaBot services, and the financial, operational, and compliance requirements that EvaBot has established for the services. The gifting automation services of EvaBot are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which EvaBot operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

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

EvaBot establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in EvaBot'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 EvaBot platform.

COMPONENTS OF THE SYSTEM

Infrastructure

The primary infrastructure used to provide EvaBot's Services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Heroku	Heroku Platform	Container runtime for web services, APIs, workers, schedulers. Includes right-scaling and self-healing to replace failed containers.
AWS	Various Services, including VPC, Elastic IP, IAM, Classic Load Balancer, RDS	Proxies for outbound data warehouse connections from EvaBot Heroku containers that allow all EvaBot traffic to emanate from a set of stable IP addresses. This allows EvaBot customers to add our IP addresses to an allowlist for their data warehouses.
AWS	S3	Temporary storage for customer data files unloaded from Redshift, MySQL, and Snowflake data warehouses

Software

The primary software used to provide EvaBot's Services system includes the following:

Primary Software		
Software	Operating System	Purpose
Ubuntu	Linux	Primary development language/runtime for all EvaBot applications
NodeJs	Linux	Web application framework used to power the EvaBot web application/sync configuration tool
MySQL	RDS	Transactional database for EvaBot data
Redis	Linux	Used to maintain the EvaBot job queue, the core of our sync engine
Bull queue	Linux	Queue management software for EvaBot job queue

People

EvaBot has employees and contractors organized into the following functional areas:

- Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

- Product Development: Product managers and software engineers who design and maintain the EvaBot sync product, including the web interface, the proprietary sync engine, the job queuing infrastructure, and all debugging tools. This team designs and implements new EvaBot functionality assesses and remediates any issues or bugs found in the EvaBot product, and architects and deploys the underlying cloud infrastructure on which EvaBot runs. This team also implements a new data warehouse and SaaS connections for the EvaBot sync engine. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team.

- Product Operations: The monitoring and maintenance of the EvaBot product (once deployed) is handled by the operations role, which involves proactively designing and deploying monitoring software and tools to help identify errors or bugs in the EvaBot product and remediate them either directly or via feedback to the product team. The operations team responds to alerts generated by our system, identifies issues with both EvaBot's sync engine and the configurations and SQL queries created by EvaBot customers, and determines the best path to resolution. Operators also ensure that syncs are performing optimally (with high throughput and low latency) and that EvaBot is using the correct cloud infrastructure and scale to maintain high sync performance. Finally, operators are responsible for responding to any potential security issues with EvaBot and notifying affected customers if applicable.

- Commercial: Individuals with commercial roles work to market, sell, and support EvaBot software. They are usually the primary point of contact for EvaBot customers. They help identify which parts of the EvaBot system are most useful to prospective customers, and what new product development or new sync connections need to be engineered to meet customer needs. In the marketing role, EvaBot employees identify best practices for automating business operations and provide that information to EvaBot customers and prospective customers via webinars, blog posts, white papers, and other channels. Finally, the EvaBot customer success team ensures that EvaBot customers can use the product effectively and without errors, by assisting EvaBot customers with onboarding into the product, helping identify useful data sources and author SQL models, and proactively identifying any issues or bugs that occur when users try to sync their data.

Data

There are three major types of data used by EvaBot:

- **Configuration Data:** Data used to configure EvaBot syncs
- **Customer Data:** Data owned by EvaBot's customers that EvaBot copies back and forth from data warehouses to SaaS applications
- **Log Data:** Logs, traces, and samples produced by the EvaBot sync engine while performing customer-configured syncs

Configuration Data is stored in EvaBot's primary PostgreSQL databases and includes:

- EvaBot customers' email addresses, names, and company names
- Credentials for accessing data warehouses, SaaS applications, and source code repositories, including usernames, passwords, OAuth tokens, and certificates
- The names of databases, schemata, tables, columns, custom objects, and custom fields in customers' data warehouses and SaaS applications
- Configuration objects that determine how data is copied between systems, including field mappings, update policies, and schedules

- Models (SQL queries) stored in EvaBot by customers to provide logical views over data before being synced.
- Audit logs covering changes to each of the above items

Configuration Data is treated as sensitive by EvaBot. It is stored with a limited lifetime when possible. Access controls limit configuration data access to each customer's EvaBot organization. Customers can invite other people in their company to access their EvaBot organization and read and write configuration data. EvaBot operators may access configuration data to troubleshoot customer issues or to gather feedback for improving the EvaBot product.

Customer Data is the most sensitive data in the EvaBot system, and EvaBot does not store it. It is currently impossible for EvaBot to sync data from data warehouses directly to SaaS applications without handling customer data, so we attempt to limit that handling as much as possible and offload as much processing to customer infrastructure as we can. When EvaBot does handle customer data, it does so using ephemeral (short-lived) worker instances and temporary storage managed by database vendors and our cloud providers. If an error occurs while running a sync, EvaBot can store a small sample of customer data in our PostgreSQL databases for ease of customer debugging. This data has a highly-limited lifetime and size, and customers can elect to disable this debugging feature. EvaBot operators are permitted to access customer data to debug complex failures in the sync engine as the result of operational issues but are encouraged to use other tools and data sources to do this debugging when possible.

Log Data is produced by the sync engine to make it easier for EvaBot operators to monitor the health of the system and track down any issues. Log data is a trace of the actions performed by the system in the course of a sync. Log data will include snapshots of **Configuration Data** at the time the sync was performed, so operators can see what the sync engine was attempting to do. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include **Customer Data** captured by automatic tracers. EvaBot endeavors to "scrub" logs of any **Customer Data** before they are persisted. Log data may be stored by vendors that EvaBot has entrusted for purposes like indexing, monitoring, and trending. Regardless of whether log data is stored within EvaBot's own databases or by vendors, it is given a limited lifetime and automatically removed.

All data types processed by EvaBot are encrypted on the wire – no networking connections used by EvaBot for any purpose will ever send unencrypted data. In addition, all **Configuration Data** and **Log Data,** as well as samples of **Customer Data** stored by EvaBot are encrypted at rest, in our own databases, our caches, and our cloud storage.

PROCESSES AND PROCEDURES

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the EvaBot policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any EvaBot team member.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow EvaBot employees physical access. At present, EvaBot does not maintain any office space, and all work is conducted remotely.

Logical Access

EvaBot employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

EvaBot infrastructure runs entirely on cloud and SaaS-based systems, and as such the resources used by employees to perform their roles are accounts and permissions within those systems. An employee can have one of their access levels to a SaaS or cloud service:

- Administrator – can alter policies and provision or de-provision users
- User – has full read/write access to the SaaS or cloud service (except for administration)
- No access

We currently do not have "read-only" roles in our SaaS or cloud applications or finer-grained policies on roles within those applications to avoid administrative complexity and friction for employees.

Roles are reviewed on an annual basis by management and the security team to ensure least-privilege access.

EvaBot identifies employees primarily by their G Suite account, which functions as our corporate directory and SSO provider. The EvaBot password policy mandates that employees and contractors use their G Suite accounts to sign into SaaS and cloud tools when supported. When G Suite sign-in is not available, employees may authenticate using a strong, unique password, which must be stored in an approved password manager.

The EvaBot G Suite tenant requires users to use a second factor for authentication. In addition, any SaaS applications used by the company that doesn't use G Suite sign-in must be configured to use a second factor when possible.

The management team is responsible for onboarding new employees. Management is responsible for provisioning G Suite and other SaaS accounts as dictated by the employee's role and performing a background check, and the employee is responsible for reviewing EvaBot's policies, completing security training, and successfully gaining access to provisioned accounts (as well as enrolling a device for second-factor authentication). These steps must be completed within 14 days of hire.

When an employee is terminated, management is responsible for removing or disabling all the employee's accounts within 3 days.

EvaBot employees may use a company-provided computer to perform their duties or may elect to "bring their own" device if that device is approved by the security team. Any computer (company-owned or BYOD) on which an EvaBot employee performs sensitive work must employ full-disk encryption and have an approved endpoint

monitoring tool installed. On employee termination, management will ensure the return of company-owned devices and handle their deprovisioning or reprovisioning based on the company's Asset Management policy.

Computer Operations – Backups

Customer data is backed up by EvaBot's operations team. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

EvaBot maintains an Incident Response Policy that gives any EvaBot employee the ability to initiate a response to a potential security incident by notifying the internal security team through several channels and assisting in classifying the severity of the incident.

External parties (customers and third-party security researchers) are also given a channel to send encrypted incident reports and responsibly disclose potential issues to the EvaBot security team.

Internally, the EvaBot operations team monitors the health of all applications, including the EvaBot web UI, sync engine, databases, and cloud storage. Monitoring includes the availability and performance of the web UI, the throughput and queuing latency of the job scheduler, and any faults or errors encountered by users while configuring EvaBot or while their data is being synced by EvaBot. Critical incidents are routed to an on-call operator who is responsible for acknowledging them within one hour; if there is no acknowledgment, the incident is escalated to the rest of the operations team.

EvaBot employs vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change Control

EvaBot maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

EvaBot has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. Our PaaS simplifies our logical network configuration by providing an effective firewall around all the EvaBot application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

Our PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

EvaBot engages an external security firm to perform quarterly vulnerability scans and annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

EvaBot does not maintain a corporate network, intranet, or VPN, but instead opts to use SaaS and cloud applications hosted on the public internet and secured by TLS connections.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Services performed by EvaBot. This report does not include the data center hosting services provided by AWS.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or another unauthorized removal of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

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

they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

EvaBot's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The EvaBot management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way EvaBot can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require EvaBot to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

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

Organizational Structure and Assignment of Authority and Responsibility

EvaBot is currently organized in a simple, flat structure in which all employees report directly to the CEO. As the team grows, management will elect to build an organizational structure that ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting upward and downward in the organizational hierarchy.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

EvaBot's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensures the service organization is operating at maximum efficiency. EvaBot's human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

EvaBot's risk assessment process identifies and manages risks that could potentially affect EvaBot's ability to provide reliable and secure services to our customers. As part of this process, EvaBot maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular EvaBot product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of EvaBot's system; as well as the nature of the components of the system result in risks that the criteria will not be met. EvaBot addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, EvaBot's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATIONS SYSTEMS

Information and communication are integral components of EvaBot's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

EvaBot uses several information and communication channels internally to share information with management, employees, contractors, and customers. EvaBot uses chat systems (Slack) and email as the primary internal and external communications channels. In addition, EvaBot communicates with customers via the Intercom customer support application.

Structured data is communicated internally via our SaaS applications (finance information in our data warehouse and Stripe) and our project management tools (Linear). Finally, EvaBot uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors control to ensure that they are operating as intended and that controls are modified as conditions change. EvaBot's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

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

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

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM IN THE LAST 12 MONTHS

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

INCIDENTS IN THE LAST 12 MONTHS

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applicable to the EvaBot Services system.

SUBSERVICE ORGANIZATIONS

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by the appropriate personnel.
		Physical access points to server locations are recorded by a closed-circuit television camera (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

EvaBot management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, EvaBot performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to EvaBot.
2. User entities are responsible for notifying EvaBot of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of EvaBot services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize EvaBot services.
6. User entities are responsible for providing EvaBot with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying EvaBot of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Test of Controls and Results Thereof

Description of Test of Controls and Results Thereof

Relevant trust services criteria and EvaBot Inc. related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if EvaBot Inc.'s controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* throughout the period December 10, 2021 to March 10, 2022.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of EvaBot Inc. activities and operations, and inspection of EvaBot Inc. documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all EvaBot Inc. controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Control Environment			
CC 1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the company's example contractor agreement to determine that it includes a code of conduct or reference to the company code of conduct.	No exceptions noted.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the company's Code of Conduct to determine that it was in place, accessible to all employees and that all employees must accept it upon hire.	No exceptions noted.
	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected documentation to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected documentation to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No exceptions noted.
CC 1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company management demonstrates a commitment to integrity and ethical values.	Inspected the ethical management questionnaire/documents to determine that the company management demonstrates a commitment to integrity and ethical values.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the most recent company organization chart to determine that it describes the organizational structure and reporting lines.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the company's security policies to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's security policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the company's security policies to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned.	No exceptions noted.
	The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Inspected documentation to determine that the company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	No exceptions noted.
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the company's Code of Conduct to determine that it was in place, accessible to all employees and that all employees must accept it upon hire.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the company's security policies to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned.	No exceptions noted.
Communication and Information			
CC 2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the infrastructure configuration to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC 2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's security policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the company's security policies to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Inspected documentation to determine that the company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually and that all employees accept these procedures when hired.	No exceptions noted.
	The company provides a description of its products and services to internal and external users.	Inspected documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company communicates system changes to authorized internal users.	Inspected the internal communication to determine that the company communicates system changes to authorized internal users.	No exceptions noted.
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected documentation to determine that the company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	No exceptions noted.
	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company website to determine that they provide guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
	The company provides a description of its products and services to internal and external users.	Inspected documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company notifies customers of critical system changes that may affect their processing.	Inspected the company website to determine that they notify customers of critical system changes that may affect their processing.	No exceptions noted.
	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company website to determine that the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Risk Assessment			
CC 3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected documentation to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No events to test.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: - these are performed on an annual basis, - threats and changes to service commitments are identified and the risks are formally assessed, - the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: - these are performed on an annual basis, - threats and changes to service commitments are identified and the risks are formally assessed, - the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually.	No exceptions noted.
	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: - these are performed on an annual basis, - threats and changes to service commitments are identified and the risks are formally assessed, - the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Monitoring Activities			
CC 4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC 4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Control Activities			
CC 5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually and that all employees accept these procedures when hired.	No exceptions noted.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually and that all employees accept these procedures when hired.	No exceptions noted.
CC 5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the data backup policy to determine that it documents requirements for backup and recovery of customer data.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected documentation to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the company's security policies to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually and that all employees accept these procedures when hired.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships.	No exceptions noted.
Logical and Physical Access			
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's data classification policy to determine that it ensures that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the company's datastores housing sensitive customer data to determine that they are encrypted at rest.	No exceptions noted.
	The company restricts privileged access to encryption keys to authorized users with business needs.	Inspected the company's Cryptography Policy to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the firewall to authorized users with business needs.	Inspected the firewall configuration to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the company's passwords for in-scope system components to determine that it is configured according to the company's policy.	No exceptions noted.
	The company restricts privileged access to the application to authorized users with business needs.	Inspected access to the application to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company restricts privileged access to databases to authorized users with business needs.	Inspected access to databases to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts access to migrate changes to production to authorized personnel.	Inspected access to migrate changes to production to determine that the company restricts privileged access to authorized personnel.	No exceptions noted.
	The company maintains a formal inventory of production system assets.	Inspected documentation to determine that the company maintains a formal inventory of production system assets.	No exceptions noted.
	The company restricts privileged access to the production network to authorized users with business needs.	Inspected access to production network to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the operating system to authorized users with business needs.	Inspected access to the operating system to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to systems and applications to determine that they use unique username and password or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as a unique SSH key.	Inspected the company's authentication to production datastores to determine that they use authorized secure authentication mechanisms, such as a unique SSH key.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC 6.4 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.	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Not Applicable - Control is implemented and maintained by subservice organizations.	No exceptions noted.
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the company's Asset Management Policy to determine that it provides guidance for proper asset disposal. Electronic media containing confidential information is purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	No exceptions noted.
	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected documentation to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's secure data transmission protocols to determine that they encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's network and system hardening standards to determine that they are reviewed at least annually based on industry best practices.	No exceptions noted.
	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the firewall rulesets to determine that it is reviewed at least annually. Required changes are tracked to completion.	No exceptions noted.
	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the company's firewall configuration to determine that they prevent unauthorized access.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's secure data transmission protocols to determine that they encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the company's mobile device management (MDM) system to determine that it is in place to centrally manage mobile devices supporting the service.	No exceptions noted.
	The company encrypts portable and removable media devices when used.	Inspected the company's portable and removable media devices to determine that they are encrypted when used.	No exceptions noted.
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the company's anti-malware technology to determine that it is configured to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
System Operations			
CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's formal policies to determine that they outline the requirements for IT-related functions such as vulnerability management and system monitoring.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: - these are performed on an annual basis, - threats and changes to service commitments are identified and the risks are formally assessed, - the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the infrastructure monitoring tool to determine that it is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the infrastructure configuration to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's formal policies to determine that they outline the requirements for IT-related functions such as vulnerability management and system monitoring.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected the company's incident response plan to determine that it is tested at least annually.	No events to test.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC 7.5 The entity identifies, develops and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No events to test.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected the company's incident response plan to determine that it is tested at least annually.	No events to test.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
Change Management			
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's network and system hardening standards to determine that they are reviewed at least annually based on industry best practices.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually.	No exceptions noted.
	The company restricts access to migrate changes to production to authorized personnel.	Inspected access to migrate changes to production to determine that the company restricts privileged access to authorized personnel.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plans to determine that they outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of EvaBot Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: - these are performed on an annual basis, - threats and changes to service commitments are identified and the risks are formally assessed, - the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
	The company has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships.	No exceptions noted.