



## **EvaBot, Inc (EvaBot)**

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability and the Suitability of the Design and Operating Effectiveness of Controls

For the period, July 01, 2022 to July 01, 2023

**(SSAE 21 - SOC 2 Type 2 Report)**



**Prepared by: Accorp Partners**

## **Table of Contents**

<b>1. Independent Service Auditor's Report.....</b>	<b>4</b>
<b>2. Management Assertion of EvaBot .....</b>	<b>8</b>
<b>3. Description of EvaBot, Inc as of throughout the audit period July 01, 2022 to July 01, 2023 .....</b>	<b>11</b>
<b>Background and Overview of Services.....</b>	<b>11</b>
<b>Significant Changes during the audit period.....</b>	<b>11</b>
<b>Subservice Organizations .....</b>	<b>11</b>
<b>Boundaries of the System .....</b>	<b>12</b>
<b>Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication.....</b>	<b>12</b>
<b>Components of the System .....</b>	<b>14</b>
<b>Applicable Trust Services Criteria and related Controls .....</b>	<b>21</b>
<b>User- Entity Control Considerations .....</b>	<b>21</b>
<b>4. Independent Service Auditor's Description of Tests of Controls and Results.....</b>	<b>23</b>
<b>5. Other Information Provided by EvaBot .....</b>	<b>44</b>



## **SECTION 1**

### **INDEPENDENT SERVICE AUDITOR'S REPORT**

# 1. Independent Service Auditor's Report

To: Management of EvaBot, Inc (EvaBot)

## Scope

We have examined the attached EvaBot, Inc (EvaBot) description of the system titled “**AI-driven Report Enablement for Enterprise**”(description) throughout the period July 01, 2022 to July 01, 2023 included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period July 01, 2022 to July 01, 2023 to provide reasonable assurance that EvaBot service commitments and system requirements would be achieved based on the trust service criteria for security, availability and confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for *Security, Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria). EvaBot has determined that Privacy Trust Services Principles are not applicable to the services provided to its client and are not included in the description.

The information included in Section 5, “Other Information Provided by EvaBot” is presented by management of EvaBot to provide additional information and is not a part of EvaBot description of its system made available to user entities during the period July 01, 2022 to July 01, 2023. Information about EvaBot business continuity planning etc. has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of EvaBot controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls

As indicated in the description, EvaBot uses Amazon Web Services (AWS) for data center services. The description in Section 3 includes only the controls of EvaBot and excludes controls of the various subservice organizations. The description also indicates that certain trust services criteria can be met only if the subservice organization’s controls, contemplated in the design of EvaBot controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center services.

## Service Organization’s Responsibilities

- EvaBot 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 the service commitments and system requirements were achieved.

EvaBot has provided the accompanying assertion titled, Management of EvaBot Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. EvaBot is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization’s service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

## **Service Auditor's Responsibilities**

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in EvaBot assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination 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, (1) the description is presented in accordance with the description criteria and (2) the controls are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description throughout the period July 01, 2022 to July 01, 2023.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. Our examination also included performing such other procedures as we considered necessary in the circumstances. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.

## **Inherent Limitations**

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

## **Opinion**

In our opinion, in all material respects, based on the description criteria described in EvaBot assertion and the applicable trust services criteria:

- a. the description fairly presents the system that was designed and implemented throughout the period July 01, 2022 to July 01, 2023.
- b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 01, 2022 to July 01, 2023, and the subservice organization and user entities applied the controls contemplated in the design of EvaBot controls throughout the period July 01, 2022 to July 01, 2023.
- c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period July 01, 2022 to July 01, 2023, and user entities and subservice organization applied the controls contemplated in the design of EvaBot controls, and those controls operated effectively throughout the period July 01, 2022 to July 01, 2023.

## **Description of Test of Controls**

The specific controls we tested and the nature, timing, and results of our tests are presented in the section 4 of our report titled "Independent Service Auditors' Description of Test of Controls and Results"

## **Restricted Use**

This report, including the description of controls and results thereof in Section 4 of this report, is intended solely for the information and use of EvaBot; user entities of EvaBot systems during some or all of the period July 01, 2022 to July 01, 2023; and those prospective user entities, independent auditors and practitioners providing services to such user entities, 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 or other parties
- Internal control and its limitations
- User entity responsibilities, Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria 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.

**Accorp Partners CPA LLC**  
**License no: PAC-FIRM-LIC-47383**  
**Date: August 24, 2023**



## **SECTION 2**

### **MANAGEMENT ASSERTION OF EVABOT**

## 2. Management Assertion of EvaBot



**EvaBot Inc. (USA)**

1601 Whipple Rd, Ste 110, Carrollton Tx – 75006 USA

July 26, 2023

We have prepared the accompanying description of EvaBot Inc.'s (EvaBot). system titled “**AI-driven Rapport Enablement for Enterprise**” throughout the period July 01, 2022 to July 01, 2023 (description), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organisation's System in a SOC 2 Report (description criteria).

The description is intended to provide users with information about **AI-driven Rapport Enablement for Enterprise** that may be useful when assessing the risks arising from interactions with EvaBot's system, particularly information about the suitability of the design of EvaBot's controls to meet the criteria related to Security, Availability and Confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

EvaBot uses Amazon AWS that provides data center services. The description includes only the controls of EvaBot and excludes controls of the subservice organizations. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organization controls contemplated in the design of EvaBot controls are suitably designed and operating effectively along with related controls at the service organization. The description does not extend to controls of the subservice organizations.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of EvaBot's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

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

a. the description fairly presents the **AI-driven Rapport Enablement for Enterprise** throughout the period July 01, 2022 to July 01, 2023, based on the following description criteria:

- i. The description contains the following information:
  - 1) The types of services provided.
  - 2) The components of the system used to provide the services, which are as follows:
    - a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
    - b) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).
    - c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
    - d) Procedures. The automated and manual procedures.
    - e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.
  - 3) The boundaries or aspects of the system covered by the description.
  - 4) For information provided to, or received from, subservice organizations or other parties,
    - a) how such information is provided or received and the role of the sub service organization






- and other parties and
- b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
- 5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
  - a) Complementary user entity controls contemplated in the design of the service organization's system.
  - b) When the inclusive method is used to present a subservice organization, controls at the subservice organization
- 6) If the service organization presents the subservice organization using the carve out method,
  - a) the nature of the services provided by the subservice organization and
  - b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
- 7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own needs.

b. the controls stated in the description were suitably designed throughout the period July 01, 2022 to July 01, 2023, to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of EvaBot controls.

Sincerely,

Ashish Kumar  
CTO  
EvaBot Inc.



**SECTION 3**  
**DESCRIPTION OF EVABOT**  
**“AI-DRIVEN RAPPORT ENABLEMENT FOR ENTERPRISE”**

**Throughout the Period**  
**July 01, 2022 to July 01, 2023**

### **3. Description of EvaBot, Inc as of throughout the audit period July 01, 2022 to July 01, 2023**

#### **Background and Overview of Services**

EvaBot platform helps 500+ CPG brands automate their end-to-end sales and distribution.

Eva AI is the sales Intelligence and engagement layer across your sales cycle that enables reps to automate the research, personalization, and engagement.

Sales teams use Eva to do multithreading and build more champions faster, driving pipeline velocity.

#### **Significant Changes during the audit period**

**No Significant changes during the audit period.**

#### **Impact of Covid and Changes to our Controls**

No change during Covid, employees connect to various IT systems directly from home. For accessing production infrastructure for administration purposes, selected employees connect to production infrastructure in AWS and data centers. The Internet has been provided to every employee working from home.

#### **Subservice Organizations**

EvaBot, Inc utilizes the following sub-service providers for data center services that are not included within the scope of this examination. However, EvaBot's responsibilities for the applications and services run at these cloud services are covered as part of the audit and in scope. The responsibility matrix is defined as part of the SLA and agreements with these sub-service organizations.

EvaBot's services are designed with the assumption that certain controls will be implemented by sub-service organizations. Such controls are called complementary sub-service organization controls. It is not feasible for all of the trust services criteria related to EvaBot's services to be solely achieved by EvaBot control procedures.

Accordingly, sub-service organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of EvaBot.

EvaBot management, along with the sub-service 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 sub-service organization controls, including the following procedures

- Holding periodic discussions with vendors and sub-service organization
- Reviewing attestation reports over services provided by vendors and sub-service organization

Monitoring external communications, such as customer complaints relevant to the services by the sub-service organization

## Boundaries of the System

The specific products and services and locations included in the scope of the report are given below. All other products, services, and locations are not included.

Products and Services in Scope
The scope of this report is limited to Technology and Development activities.

The report excludes all processes and activities that are executed outside the above locations. EvaBot, Inc has an office in Canada. The Canada office is not included in the scope of the report. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

## Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

### Control Environment

EvaBot, Inc's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team, and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at EvaBot, Inc is committed to the Information Security Management System and ensures that IT policies are communicated, understood, implemented, and maintained at all levels of the organization and regularly reviewed for continual suitability.

### Integrity and Ethical Values

EvaBot, Inc requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the company and all employees are expected to fulfil their responsibilities based on these principles and comply with all applicable laws and regulations. EvaBot, Inc promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

### Board of Directors

Business activities at EvaBot, Inc are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its founder Rabi Gupta as the Chairman & CEO. Rabi is in charge of the company's Global operations playing a key role in strategy and client management.

### Management's Philosophy and Operating Style

The Executive Management team at EvaBot, Inc assesses risks prior to venturing into business ventures and relationships. The size of EvaBot, Inc enables the executive management team to interact with operating management on a daily basis.

## **Risk Management and Risk Assessment**

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, threats to security are identified and the risk from these threats is formally assessed.

EvaBot, Inc has placed into operation a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks. The senior Management team is member of forums and core working groups in industry forums that discuss recent developments.

### **Pandemic /COVID 2019 Risks**

EvaBot, Inc has reassessed its risk with respect to Pandemic risk / COVID risks. Appropriate short-term and long-term changes have been made to impacted controls. Some of the control changes that have taken place as a result of this include:

### **Information Security Policies**

EvaBot, Inc has developed an organization-wide Information Security Policies.

Relevant and important Security Policies (IS Policies) are made available to all employees via Company Intranet or as hard copy policies to new employees. Changes to the Information Security Policies are reviewed by VP -IT and approved by CTO prior to implementation.

## **Monitoring**

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. EvaBot, Inc management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Production systems and infrastructure are monitored through service-level monitoring tools which monitor compliance with service-level commitments and agreements. Reports are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers when such commitments and agreements are not met. In addition, a self-assessment scan of vulnerabilities is performed using Symantec Antivirus software. Vulnerabilities are evaluated and remediation actions are monitored and completed. Results and recommendations for improvement are reported to management.

## **Information and Communication**

EvaBot, Inc has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based on changes and approval by management. Departmental managers monitor adherence to EvaBot, Inc policies and procedures as part of their daily activities.

EvaBot, Inc management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. For each service, there is a selected service manager who is the focal point for communication regarding the service activity. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of EvaBot, Inc's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with EvaBot, Inc employees.

### **Electronic Mail (e-Mail)**

Communication with Customer Organizations and project teams through e-Mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-Mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements.

## Components of the System

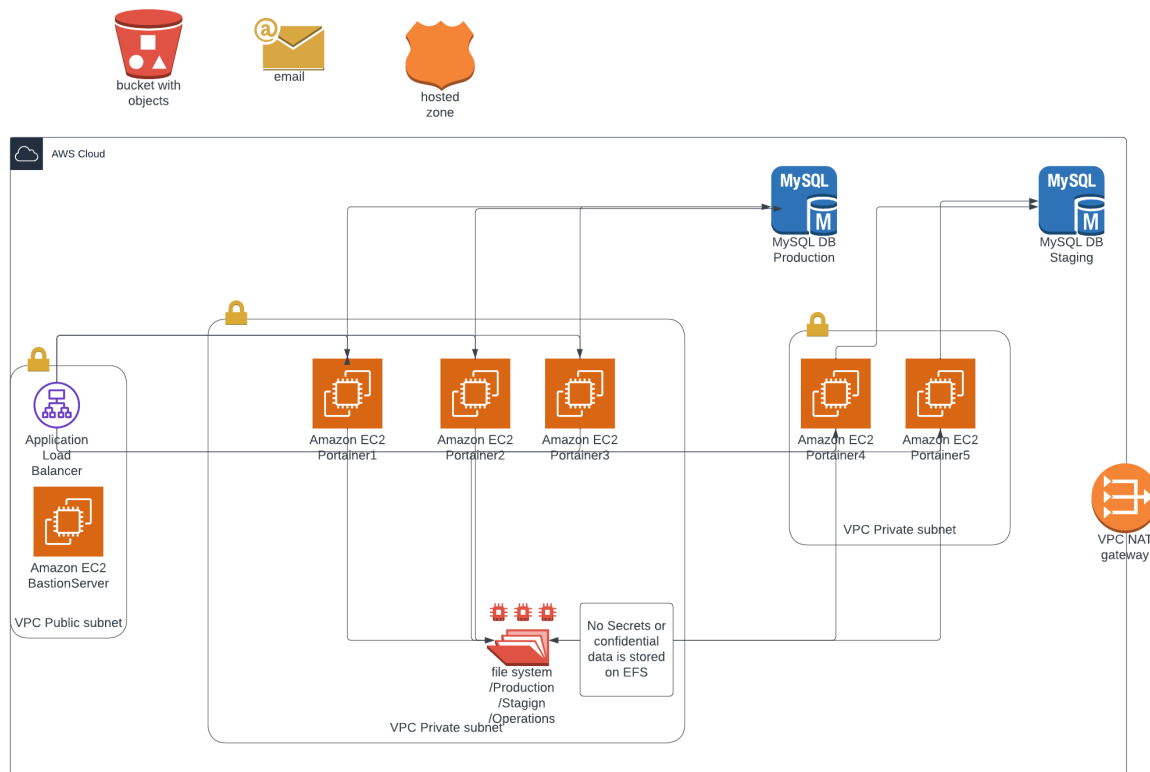
### Infrastructure

The infrastructure comprises physical and hardware components of the System, including facilities, equipment, and networks.

### Network Segmentation Overview

EvaBot, Inc offices are equipped with the latest hardware, software and networking infrastructure. Offices are linked using high-speed communication links, backed up by redundant networks.

### NETWORK DIAGRAMS



### Network Connection to Client Sites

Client application login Id and password are shared with employees for accessing their server. Clients are notified of any terminations or changes in client project personnel for people who have been provided sign-on ids.

### Physical Structure Overview

EvaBot, Inc's power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises; UPS units and backup generators supply power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly. Generators are tested periodically.

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, the warranty is checked and AMC is entered on completion of Warranty. Yearly fire drills are conducted in coordination with Admin and HR personnel. The fire drills reports are collected and analysis is made upon them.

The Media Disposal process ensures that the disposal of unwanted CDs etc. are disposed of timely to protect and maintain the security of the information and data.

## Monitoring

EvaBot, Inc has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions, and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis.

Capacity management controls are put in place to make certain EvaBot, Inc's resources are monitored, and tuned and projections are made to ensure system performance meets the expected service levels and to minimize the risk of systems failure and capacity-related issues. The addition of new information systems and facilities, upgrades, new versions, and changes are subject to formal system analysis, testing, and approval prior to acceptance.

### **Patch Management**

The security team ensures that all patches to network devices/servers operating systems are checked for stability & any availability issues & tested before applying to the production environment. Before deployment of any patches, they are tested and deployed. The patch management activity is done regularly or as and when any critical event occurs and required updates or patches are installed to ensure efficient working of the servers, desktops, and critical network devices. Operating system patches are managed and applied as they become available.

### **Vulnerability Scans & Intrusion Detection/Intrusion Prevention**

As per the Audit calendar, all the network settings are audited for any vulnerability by doing scans periodically. These scans are done by the system admin internally. Symantec Endpoint Protection is installed with the feature of scanning the device automatically and log reports are reviewed by the System Admin.

Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

All inbound and outbound e-Mails are scanned for viruses and are cleaned automatically. Anti-malware and security practices are in accordance with EvaBot, Inc Malware Protection Policy.

## People

### **Organizational Structure**

The organizational structure of EvaBot, Inc provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication and helps facilitate employees to focus on the specific business issues impacting EvaBot, Inc clients.

Rabi Gupta is responsible for oversight of EvaBot, Inc. The EvaBot, Inc site is locally managed by the following individuals/teams:

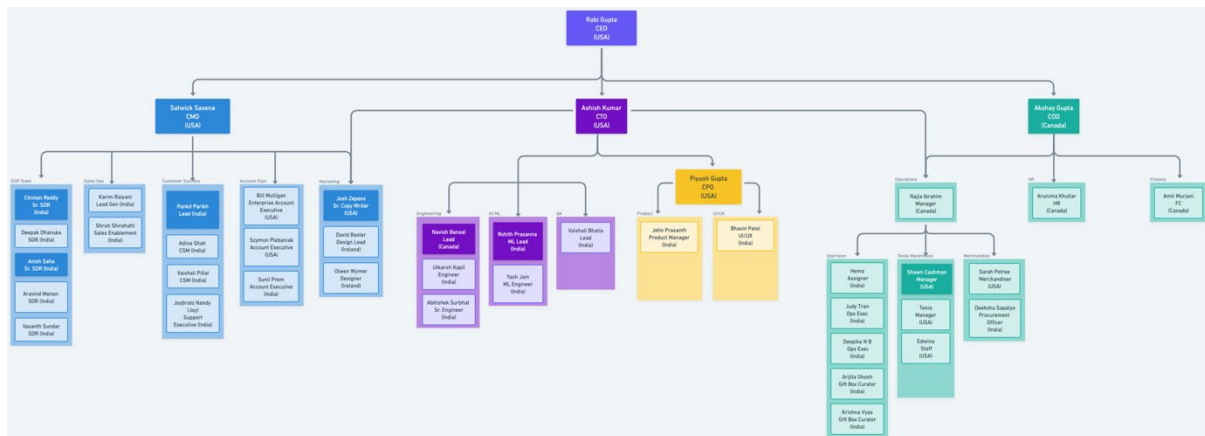
- Operations / Compliance – Akshay Gupta
- Engineering – Ashish Kumar

- Finance – Amit Murjani
- Marketing/Sales – Satwick Saxena
- Quality Assurance – Piyush Gupta
- Product Delivery - Piyush Gupta
- Information Technology – Ashish Kumar
- Compliance and Audit – Akshay Gupta
- Administration – Akshay Gupta
- Human Resources – Akshay Gupta
- Business Development – Satwick Saxena

The management team meets periodically to review business unit plans and performances. Weekly, monthly meetings and calls with senior management, and department heads are held to review operational, security, and business issues, and plans for the future.

EvaBot, Inc’s Information Security policies define and assign responsibilities/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

**EvaBot, Inc Organization Chart**



**Roles and Responsibilities**

The following are the responsibilities of key roles.

**CTO**

The CTO is in charge of the technical assets of the organization and developing safeguards to reduce the risk of breaches. Responsible for developing and implementing internal communication systems, generating IT budgets, evaluating new technologies, managing digital media assets, and executing policies.

**Commitment to competence**

EvaBot, Inc’s formal job descriptions outline the responsibilities and qualifications required for each position in the company. Training needs are identified on an ongoing basis and are determined by the current and anticipated needs of the Business. Employees are evaluated on an Annual basis to document performance levels and to identify specific skill training needs



### ***Assignment of Authority and Responsibility***

Management is responsible for the assignment of responsibility and delegation of authority within EvaBot, Inc.

### ***Human Resources Policies and Procedures***

EvaBot, Inc maintains written Human Resources Policies and Procedures. The policies and procedures describe EvaBot, Inc practices relating to hiring, training and development, performance appraisal and advancement, and termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behaviour, and competence.

The Human Resources department reviews these policies and procedures on a periodic basis to ensure they are updated to reflect changes in the organization and the operating environment. Employees are informed of these policies and procedures upon their hiring and sign an acknowledgment form confirming their receipt. Personnel policies and procedures are documented in the EvaBot, Inc Human Resources Policy.

### ***New Hire Procedures***

New employees must read EvaBot, Inc's' corporate policies and procedures and sign an acknowledgment form stating that they have read and understand them. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Background and reference checks are completed for prospective employees prior to employment over the phone. Employees are required to sign Employee Confidentiality Agreements which are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

### ***Training and Development***

On an ongoing basis, EvaBot, Inc examines its training and development needs from a business standpoint, both in terms of current needs either internal or customer driven. EvaBot, Inc compares these needs to the current skills held by its employees. On an as-needed basis, EvaBot, Inc may select certain employees to receive additional training to meet the current and anticipated needs of the organization. EvaBot, Inc also offers regular training prepared in-house to undertake training on a periodic basis on relevant topics. These trainings are attended by all technical employees of the specific department the training belongs to.

### ***Performance Evaluation***

EvaBot, Inc has a performance review and evaluation program to recognize employees for performance and contributions. EvaBot, Inc's performance evaluation process is also used to help employees improve their performance and skill levels. Employee performance reviews, promotions, and compensation adjustments are performed every 12 months. The performance evaluation is reviewed with the employee and signed by the employee, and their manager.

### ***New Employee Training***

HR coordinates to provide an information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely attendance sheets and feedback forms from employees. Employees undergo security awareness training regularly.

### ***Employee Terminations***

Termination or change in employment is being processed as per EvaBot, Inc HR-related procedures. There are clearly identified and assigned responsibilities with regard to termination or change in employment.

All employees, contractors, and third-party personnel are required to return physical and digital Identification/access tokens provided to them by EvaBot, Inc or its clients on their termination of employment or contract.

Access privileges are revoked upon termination of employment, contract, or agreement. In case of a change of employment /role, rights associated with the prior parts are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

### ***Ethical Practices***

EvaBot, Inc reinforces the importance of the integrity message and the tone starts at the top. Every employee, manager and director consistently maintain an ethical stance and supports ethical behaviour. Employees at EvaBot, Inc encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

### ***Code of Conduct and Disciplinary Action***

EvaBot, Inc has put forward a Code of Conduct and Disciplinary Process in order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. EvaBot, Inc employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the Code is prosecuted as per the defined process.

## **Procedures**

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

### ***Help Desk***

EvaBot, Inc has put in place a helpdesk function that functions out of the IT Department and an integrated helpdesk to handle problems and support requirements of users, support users in case of incidents, and manage them without disruption to EvaBot, Inc's business and ensure that changes to any component of EvaBot, Inc's information assets and infrastructure are controlled and managed in a structured manner.

All requests received at the Help Desk are classified as to their criticality and resolved within the maximum resolution time as detailed in the EvaBot, Inc Help Desk, Change Management, and Incident Response Procedure.

### ***Change Management***

EvaBot, Inc has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software, and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made to any work product. All the changes need to be subjected to a formal Change Management process.

Change Management covers any change to the Information assets and infrastructure of EvaBot, Inc and includes but is not limited to addition/ modification in the application, application components, database structure, DBMS, system and network components, policies, and procedures.

Every change to such base-lined components is governed by the change control and management procedures as outlined in the Helpdesk, Change management, and Incidence Response procedure. EvaBot, Inc's change management process requires all security patches and system and software configuration changes to be tested before deployment into Stage or Production environments.

All changes are recorded, approved, implemented, tested, and versioned before moving to the production environment. The impact of implementing every significant change is analysed and approved by the IT Head before such implementation. A sign-off is obtained from the personnel who had requested the change after implementation of the change. The effectiveness of the Change

Management process is reviewed on a monthly basis by CTO.

### ***Changes to Client System***

Change management for client systems is agreed upon with the client and is based on their requirements. All major changes must be initiated by appropriate personnel, analysed for impact, tested, and approved before deployment. Post-implementation performance will be checked as part of the change management process. All major changes to the client production system/application require approval from the Client for development to start. The development process is based on agile development with a sprint of 2 to 3 Weeks. Rigorous testing of changes requires QA testing against dummy data, integration testing, UAT, security testing, etc. based on the client's requirements. The testing strategy is agreed upon with the client and test plans and artefacts are retained.

### ***Incident Response and Management***

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. The help desk personnel study and escalate all security incidents to the designated team for further escalation/resolution. Any event related to the security of Information assets including facilities and people is termed as an Incident.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Root-cause analyses of all the incidents are performed and the root cause identified shall remedy and reported. The actions proposed from the root-cause analyses are approved by CTO

## **Logical Access**

### ***Security Authorization and Administration***

Email is sent from HR to the IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. The default access levels for different departments are defined and documented in HR/Admin policy manual. Any additional access is recommended by the line manager and approved by VP of Operations. The company has a standard configuration that is implemented across Desktops & laptops individually.

Only the IT team has access to change user profiles or give higher access. Other employees do not have local admin privileges on their desktops, only the IT team has access to install software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned to owners who are responsible for evaluating the appropriateness of access based on job roles. This is documented in Access Control Matrix.

Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to the IT team. Access to storage, backup data, systems, and media is limited to the IT team through the use of physical and logical access controls.

### ***Security Configuration***

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated by an associated password. The use of encrypted VPN channels helps to ensure that only valid users gain access to IT components. Remote access is not permitted to any employee.

Passwords are controlled through Password policy and include periodic forced changes, password

expiry, and complexity requirements. User accounts are disabled after a limited number of unsuccessful login attempts; the user is required to contact the IT Support team to reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Local administrator privilege is restricted to the IT Support Team and is not available to other users. However, where the project needs the team members to have local admin access, the respective line manager will raise a request to senior management which can approve or deny the request based on its merit.

Unattended desktops are locked during a time of inactivity. Users are required to provide their password to unlock the desktop.

### ***Administrative Level Access***

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to IT team, must be justified to and approved by VP – IT and Operations.

### **Out Bound Communication**

EvaBot, Inc development Applications are accessible in EvaBot, Inc Network. For uploading the files and communicating with the client, external internet access is required. Internet usage is restricted. The IT Team periodically reviews and recommends changes to web and protocol filtering rules. Human Resources review these recommendations and decide if any changes are to be made.

### **Confidentiality**

EvaBot, Inc classifies data as public data, internal data, and confidential data. Access to data is restricted through password-controlled folders.

Access to data is restricted to authorized applications through access control software. No confidential customer-related data is stored by the EvaBot, Inc team in the office network.

All agreements with related parties and vendors include confidentiality commitments consistent with the company's confidentiality policy (as described in IT and Security Policies).

Secure procedures are established to ensure the safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

### **Backup and Recovery of Data**

EvaBot, Inc has developed formal policies and procedures relating to backup and recovery. The backup policy is defined in the Backup Policy. Suitable backups are taken and maintained (including storing of backups offsite).

EvaBot, Inc has put in place backup processes that define the type of information to be backed up, backup cycles, and the methods of performing backup. Monthly backup copies are stored in a secure off-site location; the backup media are tested for restoration on a periodic basis to ensure the effectiveness and integrity of the backup.

The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the backup procedures.

All backup copies are tested periodically to ensure that the data and information are securely retrievable in the event of an emergency without any loss of information. Users are made aware through adequate training of their responsibilities for ensuring the backup of required data and information.

### ***Data Restoration Procedure***

Restoration is done in two cases – the primary case is when an EvaBot, Inc member makes a request

to recover some data that they might have lost. The other case when a restoration test is done is during our regular DR test. The relevant IT personnel (i.e., the backup administrator) ensures that the data is restored appropriately.

### Applicable Trust Services Criteria and related Controls

The security, availability, confidentiality and Processing Integrity trust services categories and EvaBot related controls are included in section 4 of this report, “Independent Service Auditor’s Description of Tests of Controls and Results”.

EvaBot has determined that Processing Integrity & Privacy trust services Categories are not relevant to the system.

The following criteria are not included in the system description.

<b>CC6.4</b>	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.
	AWS is responsible for ensuring the physical security of its data center and accordingly, the physical security controls under this criterion are not in scope.
<b>A1.2</b>	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
	EvaBot does not have an office or operates from a co-working space. All environmental security controls are managed by the co-working company / AWS.

### User- Entity Control Considerations

Services provided by EvaBot to user entities and the controls of EvaBot cover only a portion of the overall controls of each user entity. EvaBot controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve relating to the services outlined in this report to be achieved solely by EvaBot. This section highlights those internal control responsibilities that EvaBot believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant at user entities. Other controls may be required at user entities.

- **Contractual Arrangements**
  - User organizations are responsible for understanding and complying with their contractual obligations to EvaBot such as providing input information, review and approval of processed output and releasing any instructions.
- **Other Controls**
  - User Organizations are responsible for ensuring end customer privacy.
  - User Organizations are responsible for ensuring that complete, accurate and timely information is provided to EvaBot for processing.
  - User Organizations are responsible for their network security policy and access management for their networks, application & data.
  - User Organizations are responsible for working with EvaBot to jointly establish service levels and revise the same based on changes in business conditions



## **SECTION 4**

### **INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS**

#### 4. Independent Service Auditor's Description of Tests of Controls and Results

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	<b>Control environment</b>		
<b>CC1.1</b>	<b>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</b>		
	Company has Information security related policies and procedures that describes information security processes, practices and organization.	Inspected ISMS Policies and Procedures and related IT Policies to determine that these are documented.	No Exceptions noted
	The Company has a mission and vision statements. Additionally, the entity has developed a clearly articulated statement of ethical values that is understood at all levels of the organization.	Inspected the mission/ vision statement of the company to determine that the vision statement is documented.	No Exceptions noted
	The Company has approved code of conduct that is applied across the entity. The Code of Conduct outlines strict disciplinary consequences for violation of code of conduct	Inspected the hosting of Code of conduct on the Training Portal and Shared Directory of company to determine that the code of conduct is accessible to all users.	No Exceptions noted
	All new employees are provided training or a copy of the code of conduct. New employees sign off that they have read this document online.  Existing employees, on an annual basis, undergo refresher training on Company's policies on code of conduct. COC posted on the GRC Training Portal	Selected a sample of new joiners and inspected the training records to determine that all new joiners accept code of conduct.  Selected a sample of existing employees and inspected the screenshot of the training records to determine that all existing employees also review and accept code of conduct done.	No Exceptions noted
	Performance appraisals are performed at least annually.	Enquired with Head HR that performance appraisals are carried out on an annual basis.	No Exceptions noted
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	Inspected a sample of vendor agreements to determine that these contained clauses relating to confidentiality of data and commitments relating to availability.	No Exceptions noted
	The entity has code of conduct that establishes standards and guidelines for personnel ethical behaviour.  Personnel are required to read and accept the entity's code of conduct	Inspected the code of conduct policies to determine that the entity has established standards and guidelines for personnel ethical behaviour including code of conduct.	No Exceptions noted
	All new employees have to read and sign the Confidentiality Agreement/NDA upon joining.	Selected a sample of new joiners and inspected personnel file to determine that Confidentiality agreements / NDA are signed.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	<p>Customer can provide their issues, complaints or feedback through email to Business Heads.</p> <p>Employees can raise their complaints and grievances to HR.</p>	<p>Inspected customer resolution clauses in a sample of customer Master Service Agreement (MSA) and determined that customer have a mechanism to communicate with the company.</p>	<p>No Exceptions noted</p>
<b>CC1.2</b>	<b>COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</b>		
	<p>Management Review Meetings headed by CTO are held every quarter to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.</p>	<p>Selected a sample of MRM meetings held and inspected the minutes to determine that MRM are held on a periodic basis.</p>	<p>No Exceptions noted</p>
<b>CC1.3</b>	<b>COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</b>		
	<p>Organization charts are established that depicts authority, reporting lines and responsibilities for management of its information systems.</p> <p>These charts are communicated to employees and are updated as needed</p>	<p>Inspected the organization chart for an understanding of the hierarchy.</p> <p>Enquired with Management to determine that organisation charts are updated periodically.</p>	<p>No Exceptions noted</p>
	<p>Company has Information security related policies and procedures that describes information security processes, practices and organization.</p>	<p>Inspected ISMS Policies and Procedures and related IT Policies to determine that these are documented approved by CTO.</p>	<p>No Exceptions noted</p>
	<p>Information Security Policy &amp; Procedures related to HR policies are reviewed and approved by the Management at least annually.</p>	<p>Inspected ISMS Manual and related IT Policies to determine that changes during the audit period are approved by Director</p>	<p>No Exceptions noted</p>
	<p>The responsibility of managing Information Security is assigned to CTO.</p> <p>Allocation of information security responsibility is documented in CTO</p>	<p>Inspected Policy Approval Form to determine that Information Security activities are responsibility of CTO.</p>	<p>No Exceptions noted</p>
<b>CC1.4</b>	<b>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</b>		
	<p>The company has documented HR Policies and procedures including recruitment, training and exit procedures.</p>	<p>Inspected the HR Policies and procedures to determine that these are documented</p>	<p>No Exceptions noted</p>
	<p>Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.</p>	<p>Inspected the HR Policies and a sample of related job description to determine that requirements for each role are documented and are evaluated as part of the hiring process.</p> <p>Selected a sample of new joiners and inspected the personnel files for the</p>	<p>No Exceptions noted</p>



Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
		competency checks such as Assessment Tests.	
	New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms.	Selected a sample of new joiners and inspected the offer letter to determine that new joiners accept the terms of employment.	No Exceptions noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected a sample of HR meeting minutes to determine that resource planning is reviewed periodically.	No Exceptions noted
	Internal HR Reference checks are conducted by the HR team or the hiring manager through document verification and reference checks with the former colleagues or managers provided in the resume.	Selected a sample of new joiners and inspected personnel files to determine that internal HR reference checks are carried out as per defined policies.	No Exceptions noted
	Company does not employ contractors.	Enquired with HR Head that the company does not employ contract staff.	No Exceptions noted
	Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position	Enquired with HR Head that all new employees undergo induction training.	No Exceptions noted
	The induction training given through an online Portal GRC Training Portal and administered by HR includes information security training. In this training the HR, physical access and security policies are explained.	Inspected Online Portal GRC Training Portal to ensure that it includes policies on security and also covers identification and report of security breaches  Selected a sample of new joiners and inspected the induction attendance/ training records to determine that new joiners undergo information security trainings.	No Exceptions noted
	An awareness refresher training is provided to all employees on at least annual basis.	Inspected training records for a sample of existing employees and determined that annual training was completed.	No Exceptions noted
<b>CC1.5</b>	<b>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</b>		
	Roles and responsibilities are defined in written job descriptions and communicated to employees and their managers	Inspected the IT policies / Roles and responsibilities document to determine that roles and responsibilities are defined.	No Exceptions noted
	Job descriptions are reviewed by entity management on an annual basis as part of performance appraisals.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised as and when required.	No Exceptions noted
	Employees and contractors acknowledge the Code of Conduct annually.	Inspected the GRC Training Portal screens records for acceptance for code of conduct by employees to determine	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
		that all existing employees review and accept Code of Conduct online.	
	Performance appraisals are performed at least annually.	Inspected a sample of performance appraisals for existing employees to determine that performance appraisals are performed at least annually	No Exceptions noted
	<b>Communication and Information</b>		
<b>CC2.1</b>	<b>COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</b>		
	Internal audits are performed, results are communicated and corrective actions monitored.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions noted
	A standing meeting is carried out weekly to hold department discussion and status updates.	Enquired with management that weekly departmental meeting minutes are held.	No Exceptions noted
<b>CC2.2</b>	<b>COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</b>		
	System boundaries in terms of logical and physical boundaries are documented. Network diagrams are in place.  System Boundaries are shared with the customers when it is required.	Inspected the Information Security policies and the network diagram to determine that the Company has defined system boundaries.	No Exceptions noted
	Customer responsibilities and appropriate system descriptions are provided in client contracts.	Inspected Client contracts for terms related to brief requirements of the system and customer responsibilities	No Exceptions noted
	Security policies are published on shared drive and GRC Training Portal Training Portal.	Inspected the shared drive and GRC Training Portal Training Portal to determine that IT security policies available to internal users.	No Exceptions noted
	An organizational wide incident management process is in place	Inspected ISMS / Information Security Policies to determine that incident management process is documented.	No Exceptions noted
	Entity communicates its commitment to security as a top priority for its customers via contracts and website pages	Inspected a sample of customer and vendor contracts to determine that it contains clauses relating to confidentiality.	No Exceptions noted
	All system changes that affect internal and external users are communicated in a timely manner	Inspected ISMS and related change management policies to determine how changes to system are communicated to users.	No Exceptions noted
	CTO is responsible for decisions regarding changes in confidentiality practices and commitments.	Enquired with CTO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Operations team communicates these changes to the customers.		
	New employees hired at senior levels are communicated to stakeholders by HR through Email	Inspected a sample of HR emails / periodic management meetings to determine that senior management hires are communicated internally and if necessary, externally.  Enquired that there was no senior level management hiring during the period for senior employees.	No Exceptions noted
<b>CC2.3</b>	<b>COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</b>		
	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / MSA	Inspected sample of Client contracts / MSA and determined that terms related to delivery of services such as availability and confidentiality are covered.	No Exceptions noted
	Security policies are published on GRC Training Portal and Shared Directory Server.	Inspected the GRC Training Portal and Shared Directory Server to determine that IT security policies available to internal users.	No Exceptions noted
	The induction training given through an online Portal GRC Training Portal and administered by HR includes information security training. In this training the HR, physical access and security policies are explained.	Inspected Online Portal GRC Training Portal to ensure that it includes policies on security and also covers identification and report of security breaches  Selected a sample of new joiners and inspected the induction attendance/ training records to determine that new joiners undergo information security trainings.	No Exceptions noted
	Customer responsibilities are described in client contracts / MSA / SLA	Inspected a sample of client contracts / MSA to determine explicit responsibilities of customer	No Exceptions noted
	Users are informed of the process for reporting complaints and security breaches during induction Security Training.	Selected a sample of new employees and inspected evidence to determine that they attended Security Training during induction.	No Exceptions noted
	Customer can provide their issues, complaints or feedback through email to Business Heads.  Employees can raise their complaints and grievances to HR.	Inspected customer resolution clauses in a sample of customer Master Service Agreement (MSA) and determined that customer have a mechanism to communicate with the company.	No Exceptions noted
	A client escalation matrix is in place to ensure that communication channels for external users are available.	Inspected the client escalation mechanism to determine that it is implemented	No Exceptions noted
	Customer responsibilities are described in the customer contracts and in system documentation	Inspected a sample of customer MSA for the roles and responsibilities and determined that roles and responsibilities are clearly defined. .	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	CTO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team communicates these changes to the customers.	Enquired with CTO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No Exceptions noted
	Changes to system boundaries, network systems are communicated to clients, if it impacts their operations	Enquired with CTO and IT Head that changes to system boundaries are communicated internally and externally	No Exceptions noted
	Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	Enquired with CTO that major incidents are reported to clients along with root cause.	No Exceptions noted
<b>Risk Assessment</b>			
<b>CC3.1</b>	<b>COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</b>		
	Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process that includes risk assessment scales.	No Exceptions noted
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No Exceptions noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected a sample of HR meeting minutes to determine that resource planning is reviewed periodically.	No Exceptions noted
<b>CC3.2</b>	<b>COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.</b>		
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No Exceptions noted
	A risk assessment is performed annually or whenever there are changes in security posture.  As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment performed during the audit period to determine updation of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions noted
	The Risk and Compliance team monitors the environment of internal control and identifies significant changes that have occurred.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions noted
	Identified risks are rated and get prioritized based on their Probability, Impact and the existing control measures.	Inspected Risk Assessment performed during the year to determine identified risks are rated	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Risk Mitigation Plans and action trackers are in place to respond to risks.	Inspected the risk mitigation plans/ risk tracker to determine that action trackers are in place to mitigate risks.	No Exceptions noted
	All information assets are identified in an asset inventory	Inspected the asset register / hardware list to determine that all assets are recorded.	No Exceptions noted
	Technical vulnerability management is implemented using third party. Critical threats are reviewed and resolved timely.	Inspected a sample of VA scans to determine that the scans were executed.	No Exceptions noted
<b>CC3.3</b>	<b>COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</b>		
	List of all hardware is maintained as part of asset register.	Inspected the asset register / hardware list to determine that all assets are recorded.	No Exceptions noted
	Company has defined a formal risk management process for evaluating risks based on identified Probability, threats and mitigating controls.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No Exceptions noted
<b>CC3.4</b>	<b>COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</b>		
	Whenever new products or services are added or its business model changes, a risk assessment is carried out for the new service.	Inspected sample of Risk Assessment performed during the audit period to determine that risk assessment is carried out for recently introduced products / services.	No Exceptions noted
	Emerging technology and system changes are considered when performing risk assessment	Inspected sample of Risk Assessment performed during the audit period to determine that risk assessment is carried out for emerging technology and system changes.	No Exceptions noted
<b>Monitoring Activities</b>			
<b>CC4.1</b>	<b>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.</b>		
	The internal audit function conducts system security reviews periodically. Results and recommendations for improvement are reported to management.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions noted
	IT system access is reviewed on a Quarterly basis.	Inspected the information security policies containing access controls to determine that these are documented.  Inspected a sample of system access review reports to determine that access rights are reviewed regularly and user access lists are reconciled against active HR records.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Vulnerability assessment & penetration tests are performed quarterly by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions noted
<b>CC4.2</b>	<b>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.</b>		
	Vulnerability assessment & penetration tests are performed quarterly by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions noted
	Results of the vulnerabilities are reviewed by the management	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions noted
<b>Control Activities</b>			
<b>CC5.1</b>	<b>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.</b>		
	Vulnerability assessment & penetration tests are performed quarterly by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions noted
	Control Activities are defined at entity level and at departmental levels.	Inspected the control framework and related policies to determine that controls are defined at entity level as well as departmental levels	No Exceptions noted
<b>CC5.2</b>	<b>COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</b>		
	Vulnerability assessment & penetration tests are performed quarterly by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions noted
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No Exceptions noted
<b>CC5.3</b>	<b>COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</b>		
	All policies are reviewed at least every year to ensure that these are current and in line with the current business.	Selected a sample of IT Policies as well as other departmental policies to determine that the last review date was within the last 12 months.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Significant policies and procedures are uploaded to the Shared Drive and GRC Training Portal Training Portal and available for all employees that require access to these policies/procedures.	Inspected the Shared Drive and GRC Training Portal Training Portal to determine that IT security policies as well as other business function policies are available to internal users.	No Exceptions noted
	All policies and procedures clearly define the roles, responsibilities and accountability for executing policies and procedures.	Inspected ISMS Policies and Procedures to determine that policies and procedures clearly define the roles, responsibilities and accountability for executing policies and procedures.	No Exceptions noted
<b>Logical and Physical Access Controls</b>			
<b>CC6.1</b>	<b>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.</b>		
	Company has documented procedure for logical access controls	Inspected the access control policy and procedure and determined that these are documented.	No Exceptions noted
	Access is granted on least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on least privileges basis as default and any additional access needs to be approved.	No Exceptions noted
	Company has established hardening standards production infrastructure that include requirements for implementation of security groups, access control, configuration settings, and standardized policies.	Inspected IT policies and procedures to determine that hardening standards have been established.	No Exceptions noted
	Production hosts and Security Groups (which are the equivalent of Firewalls) are hardened according to Industry best practices. Only the required ports are opened for inbound access at the load balancer level.	Inspected AWS settings to determine that VPC has been setup and all production server are within the private subnet.	No Exceptions noted
	Physical and logical diagrams of networking devices for office network include routers, firewalls, switches and servers, including wireless, are documented.	Inspected the system diagrams and networking diagrams to determine that these are documented.	No Exceptions noted
	Company does not allow customers or external users to access its systems.	Enquired with IT team that external users cannot access company's network systems	No Exceptions noted
	The company does not have an office network / Active Directory etc.  All user machines are independently monitored by the IT team on a periodic basis. Local Group policies require authentication on user machines through a password policy.	Inquired with Head IT that the company does not have Active Directory.  Inspected the periodic monitoring records for a sample month/quarter to determine that the IT team monitors the user devices on a periodic basis.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Cloud infrastructure is configured to use the AWS's identity and access management system (IAM). Relevant groups have been added in IAM.	Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the production group has access to production resources.	No Exceptions noted
	Direct access to AWS cloud infrastructure is possible only through encrypted SSH access by the IT team.	<p>Inspected the properties of VPC security group and determined that the inbound connection to instances in the VPC is set to be accessed by an SSH connection.</p> <p>Inspected SSH settings in SSH client to determine that encrypted SSH key is required for connecting to AWS / Cloud infrastructure.</p>	No Exceptions noted
	For AWS console access, Multi Factor Authentication is implemented.	Inspected the user settings in AWS console for the production group members to determine that multifactor authentication has been enabled.	No Exceptions noted
	<p>The Company has a remote working policy as part of Access Control Policy that requires that external access is granted on a need basis.</p> <p>Currently, as a default, external access by employees is prohibited.</p>	<p>Enquired with IT staff about external access by employees and determined that external access is not allowed.</p> <p>Inspected Information Security Policy and determined that Company has remote working policies that are documented</p>	No Exceptions noted
	The IT department maintains an up-to-date listing of all software.	<p>Inspected the software list maintained by the IT to ensure that it is up to date.</p> <p>Inspected the software installed in sample desktop to ascertain that current versions are installed.</p>	No Exceptions noted
	All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed.	Inspected the asset register and determined that assets and their owners are clearly documented.	No Exceptions noted
	<p>Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Management.</p> <p>Privileged access is authorised by CTO and reviewed by IT on a periodic basis.</p>	Inspected screenshots of AWS IAM to determine that administrator privileges for the cloud were limited to IT team.	No Exceptions noted
	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing.	No Exceptions noted
	Password policy is set at the Local Policy level. Passwords are manually set on each user's desktops by the IT team. These are 7 characters in length with complexity enabled.	Inquired with the IT Head that passwords are manually set by the IT team and are reset every 45-60 days by the IT team.	No Exceptions noted



Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	<p>Passwords are reset by the IT team manually every 45-60 days by going to each user's desktop and resetting the passwords. On the next login, the user in the presence of the IT team will reset the password.</p>		
	<p>Employees do not have access to printers or any other output device. Printer access is given for few teams such as HR and few after approval by CTO.</p>	<p>Enquired with IT team that no printer access is given to employees and determined based on enquiry that output access is controlled.</p>	<p>No Exceptions noted</p>
	<p>All confidential data is classified as per the data classification policy</p>	<p>Inspected information security policies to determine that data classification policies are documented.</p>	<p>No Exceptions noted</p>
<b>CC6.2</b>	<p><b>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.</b></p>		
	<p>On the day of joining, HR will send a mail to IT Helpdesk providing the details of the new joiners. The IT then provides necessary access as per request</p> <p>Employee user accounts are removed from various application and network system as of the last date of employment manually based on access revocation request sent by HR department.</p>	<p>Inspected the Access Control procedure and determined that granting, modifying or deactivating access is only done against written authorization.</p> <p>Inspected access request forms / emails for a sample of employees to determine that written authorisation is in place.</p> <p>Inspected access revocation request /exit checklist for a sample of employees to determine that written authorisation for deactivation is in place.</p>	<p>No Exceptions noted</p>
	<p>When an employee leaves the organization, the employee's manager initiates the Exit Process. HR informs respective teams / IT team within 24 hours to deactivate/delete the user ID from the email system and all applications.</p> <p>An exit checklist is used to ensure compliance with termination procedures.</p>	<p>Selected a sample of exited users and inspected Email from HR to IT and Exit Checklist to determine that the exit process and related account deactivation is as per defined procedures.</p> <p>Inspected the IAM screens to determine that the exited user has disabled status in IAM.</p>	<p>No Exceptions noted</p>
	<p>HR team raises a ticket in Saastematic Tool or email for the user deactivation list to IT team within 24 hours from the time an employee is terminated or the last working day.</p>	<p>Inspected access revocation email from and HR to IT for sample off-boarded employees; verified their disabled status in IAM.</p>	<p>No Exceptions noted</p>
	<p>Company does not employ contractors in its offices.</p>	<p>Enquired with IT staff about access to non-employees to determine that there are no contractors.</p>	<p>No Exceptions noted</p>
<b>CC6.3</b>	<p><b>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,</b></p>		

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	<b>considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.</b>		
	A role-based security process has been defined within AWS infrastructure based on job requirements.	Inspected the AWS console screens to determine that security groups based on departments and roles have been defined	No Exceptions noted
	Company does not allow reactivation of ID belonging to an exited employee.	Inspected IT policy about reactivation of IDs and determined that it is prohibited.	No Exceptions noted
	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing.	No Exceptions noted
<b>CC6.4</b>	<b>The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</b>		
	All customer data is on AWS and there is no critical data in EvaBot offices. Accordingly, CC6.4 is not applicable.	Not applicable	Not Applicable
<b>CC6.5</b>	<b>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.</b>		
	Media Handling Policy documented as part of Asset Management Policy is implemented for procedures relating to disposal of information assets / equipment	Inspected the media handling policy to determine that it is documented.	No Exceptions noted
	All data is erased from laptops and other media prior to destruction disposal	Inspected the media handling policy to determine that for all media that is disposed off, data is erased from these prior to disposal.	No Exceptions noted
<b>CC6.6</b>	<b>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</b>		
	There are no firewalls in the office since all users connect directly to cloud infrastructure to do all of their work. Employees connect to the local Wi-Fi networks securely from their laptops.	Inspected the network diagram to determine that the company does not have a firewall.	No Exceptions noted
	The production system at AWS is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all Production system hosted at AWS.  Only limited employees in the production group have access to production servers using SSH through a NAT gateway.	Inspected AWS settings to determine that VPC has been setup and direct access to production instances is only through 2048-bit SSH keys.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Access to modify Security group rules is restricted by management.	Inspected the user list on IAM to determine that access to modify security group rules is restricted to Administrators/IT team.	No Exceptions noted
	Data is stored in encrypted format using software supporting the AES.	Inspected evidence of encryption of data storage.	No Exceptions noted
	Use of removable media is prohibited by policy except when authorized by management.	<p>Inspected DLP policies for removable media.</p> <p>Observed a sample of computers and determined that USB sticks are not read.</p>	<p>Exceptions noted</p> <p>USB Drives are not blocked for users.</p> <p>Management response –</p> <p>USB drives are not blocked for users: We do not believe that blocking USB drives would materially alter exfiltration risk, and blocking all file-sharing mechanisms (wireless and physical) would make doing business materially more difficult with little security benefit beyond the contractual and policy-based protections in place, so we choose not to enforce this.</p>
	Connections to the AWS-hosted servers are through authenticated SSH sessions or authenticated secure browser session using HTTPS.	Inspected AWS settings to determine that direct access to production instances is only through 2048-bit SSH keys.	No Exceptions noted
<b>CC6.7</b>	<b>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.</b>		
	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policies to determine that transmission of sensitive information over the internet happens only when the information is encrypted.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	External users access applications hosted at cloud infrastructure AWS through secure https with SSL/TLS certificates.	Inspected evidence for implementation of https encryption to determine that secure https connections are used.	No Exceptions noted
	<p>The production system at AWS is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all Production system hosted at AWS.</p> <p>Database access is governed by security group policies and login credentials. Production database can only be accessed from production machines.</p>	Inspected AWS settings to determine that VPC has been setup for application & database and that all production servers are within the private subnet and direct access to EC2 instances is only through 2048-bit SSH keys.	No Exceptions noted
	Use of removable media is prohibited by policy except when authorized by management	<p>Inspected DLP policies for removable media.</p> <p>Observed a sample of computers and determined that USB sticks are not read.</p>	<p>Exceptions noted</p> <p>USB Drives are not blocked for users.</p> <p>Management response - USB drives are not blocked for users: We do not believe that blocking USB drives would materially alter exfiltration risk, and blocking all file-sharing mechanisms (wireless and physical) would make doing business materially more difficult with little security benefit beyond the contractual and policy-based protections in place, so we choose not to enforce this.</p>
	Backup media are encrypted during creation.	Enquired with Head IT that all backup media are encrypted during creation	No Exceptions noted
<b>CC6.8</b>	<b>The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</b>		
	Antivirus software Seqrite is installed on workstations and laptops. This system provides antivirus system	<p>Inspected a sample of desktops and servers and determined that antivirus is installed and signature files were updated.</p> <p>Inspected the antivirus/firewall console for</p>	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	scans, content filtering and endpoint protection.	configuration details about updating and alerts.	
	Signature files are updated daily. Antivirus console provides compliance reports about non-updated machines.	Inspected a query report from the console showing unupdated computers and determined that there were no such cases.  Inspected the antivirus/firewall console for configuration details about updating and alerts.	No Exceptions noted
	The ability to install software on workstations and laptops is restricted to IT support personnel through domain policies.  Local admin access is granted on a need-based approval from CTO.	Inspected the Information Security Policies to determine that users are not allowed to install any software.  Inspected domain policies for local admin and determined that is it disabled for local users.	No Exceptions noted
	Any viruses discovered are reported to IT team either by the antivirus system or by the affected employees.	Inspected the antivirus console for configuration details about updating and alerts.  Inspected the security training pack for the instructions to employee about virus incidence reporting.	No Exceptions noted
<b>System Operations</b>			
<b>CC7.1</b>	<b>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.</b>		
	Management has defined configuration standards and hardening standards.	Inspected IT policies and procedures to determine that hardening standards have been established.	No Exceptions noted
	Penetration testing is performed by on a periodic basis	Inspected the latest penetration testing report to determine that periodic penetration tests are carried out.	No Exceptions noted
<b>CC7.2</b>	<b>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 analysed to determine whether they represent security events.</b>		
	Hardening Checklists are in place for hardening of IT infrastructure/desktops.	Inspected the standards for hardening of IT Infrastructure and desktops.  Inspected a sample of desktops to ensure that they were configured as per the hardening standards.	No Exceptions noted
	IT team receive requests for support through phones, emails and Saastematic Tool Tickets, which may include requests to reset user passwords etc.	Inspected a sample of IT support ticket emails reported by users to determine that support tickets are logged as Saastematic Tool Tickets.	No Exceptions noted
	Vulnerability monitoring scans are performed on a periodic basis.	Inspected a sample of VA scans to determine that the scans were executed.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Management takes appropriate action based on the results of the scans.	Inspected relevant evidence and management meeting minutes to determine that vulnerabilities were tracked and closed.	
<b>CC7.3</b>	<b>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.</b>		
	A formal, defined incident management process is documented in Information Security Policies for evaluating reported events.	Inspected ISMS / Information Security Policies to determine that incident management process is documented.	No Exceptions noted
	Incidents are reported to the IT team. These are tracked through an incident management tool.	Inspected the screenshot of the incident management tool to determine that incidents are tracked.	No Exceptions noted
	Reported incidents are logged as tickets and include the following details  Severity Data and Time of incident Details Status Root Cause (High severity incidents only)	Inspected a sample of incident report to determine that incidents covered severity, date, time, details, status and root cause (if major) to determine that incidents are handled as per defined process.	No exceptions noted  There were no reported incidents.
<b>CC7.4</b>	<b>The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</b>		
	All security incidents are also reviewed and monitored by the CTO. Corrective and preventive actions are completed for incidents.	Inspected minutes of IT for discussion on incidents.	No exceptions noted  There were no reported incidents and hence no discussion in the meetings.
	Change management requests are opened for events that require permanent fixes.	Inspected Incident Management Procedure and determined that for some incidents, change requests are opened as part of resolution.	No Exceptions noted
	All incidents are evaluated and necessary action taken to close the threat / vulnerability	Inspected the screenshot of the incident management tool to determine that incidents are tracked.	No Exceptions noted
	HR policies include code of conduct and disciplinary policy for employee misconduct.	Inspected the Employee Handbook for Code of Conduct and Disciplinary Policy	No Exceptions noted
<b>CC7.5</b>	<b>The entity identifies, develops, and implements activities to recover from identified security incidents.</b>		
	All incidents are evaluated and necessary action taken to close the threat / vulnerability	Inspected minutes of Meeting for discussion on incidents.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Root cause analysis is performed for major incidents.	Inspected a sample of incident reports to determine that root cause analysis is performed for critical / major incidents.	No Exceptions noted
<b>Change Management</b>			
<b>CC8.1</b>	<b>The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</b>		
	All change requests must be peer reviewed by another programmer for consistency purposes.	Enquired with management to determine that formal code review is performed by a peer programmer.	No Exceptions noted
	System and regression testing are prepared by the testing department using approved test plans and test data.	Inspected test plans for sample of releases to determine that test plans included steps for regression testing, security testing	No Exceptions noted
	Software code is maintained in GitHub.	Inspected screenshot of GitHub to determine that software code is maintained in GitHub.	No Exceptions noted
	Software development changes are tested through unit testing and QA testing followed by UAT. Each of these activities are captured & monitored in change requests.  Test plans used for testing QA team.	Inspected a sample of change requests for software development to determine that QA/UAT testing is carried out.	No Exceptions noted
	There is a formal release process for releasing builds. Release notes contain what all is released in the release. The testing team does the complete testing of the release. Releases are tracked and Approved in GitHub.	Selected a sample of releases during the audit period and inspected the release notes and the related approval to determine that all releases are tested and approved before deployment	No Exceptions noted
	Separate environments are used for development, testing, and production.  Developers do not have the ability to make changes to software in testing or production.	Enquired with the management to determine that separate environments are maintained for development, testing and production and also to understand about process to carry out major changes.	No Exceptions noted
	All change requests are submitted with implementation and rollback plans.	Inspected a sample of change requests to determine that they had rollback plans included.	No Exceptions noted
	Changes are communicated to the appropriate client and user community if the change has any potential impact on the user base.	Enquired with management that changes are communicated to clients and end users if it has impact on those users.	No Exceptions noted
	The change management process has defined roles and assignments thereby providing segregation of roles in the change management process.	Inspected the Change Management Policy and Procedures to determine that these define segregation of roles for change management.	No Exceptions noted

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	Entity has defined its change management and approval processes in its information security policies.	Inspected Information Security Policy and determined that change management policy and procedures are defined.	No Exceptions noted
	Software design and development change procedures are documented in the SDLC Process in GitHub.	Inspected the SDLC procedures in GitHub to determine that software design and development change procedures are documented.	No Exceptions noted
	All change requests are logged and change request ticket created.  Changes are approved by change advisory board	Selected a sample of change requests to determine that these are logged and that changes are approved by Change Advisory Board.	No Exceptions noted
	A risk assessment is performed on a periodic basis. The risk assessment includes identifying potential threats and assessing the risks associated with identified.  Change requests are created based on the identified needs.	Inspected the risk management procedures to determine if change requests are created based on identified needs.	No Exceptions noted
	A process exists to manage emergency changes.  Emergency changes, due to their urgent nature, may be performed without prior review.	Inspected Change Management policy to determine that the policy considers process to manage emergency changes	No Exceptions noted
	Data for testing is manually generated before being used in testing.	Enquired with management that test data is created by the QA Team and no actual data is used in testing	No Exceptions noted
<b>Risk Mitigation</b>			
<b>CC9.1</b>	<b>The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</b>		
	Entity has a documented BCP and DR guideline to be used in the event of an event necessitating systems infrastructure recovery.	Inspected the policies and procedures relating to disaster recovery & Business Continuity plans to determine that a plan and procedure has been documented with clear responsibilities on those required to respond.	No Exceptions noted
	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the Business Continuity Planning Policy and determined that BCP plans are tested at least annually.	No Exceptions noted
<b>CC9.2</b>	<b>The entity assesses and manages risks associated with vendors and business partners.</b>		
	New Third-Party Service Providers are selected based on a Vendor Selection Process. Security risk assessment is a key part of the vendor selection process.  Company requires all key subservices to be compliant with security	Enquired with Management that vendors and third-party service providers are selected based on a vendor due diligence.  Enquired with Management that there	No Exceptions noted



Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	certifications and attestations such as ISO 27001, SOC1 or SOC2.	was no material third party vendor that was onboarded during the audit period.	
	Company obtains and reviews compliance reports and certificates such as PCI DSS, ISO 27001, SOC1 or SOC2 for its key vendors. Opinion section and relevant controls are reviewed for any exceptions. This is part of vendor monitoring.	Inspected sample certification and attestation reports of Company's vendors to determine that the company receives such reports that are used in monitoring controls.	No Exceptions noted
	All customer & vendor contracts have terms related to confidentiality.	Inspected a sample of customer and vendor contracts to determine that it contains clauses relating to confidentiality.	No Exceptions noted
	A confidentiality agreement is signed by all employee at the time of joining. In addition, NDAs are signed with third parties wherever required.	Inspected the confidentiality agreement template to determine that agreements include terms on confidentiality and non-disclosure.	No Exceptions noted
	Vendor systems are subject to review as part of the vendor risk selection.  AWS is the sole service provider that provides data center services. Attestation reports (SOC 2SM reports) are obtained from AWS and evaluated when available.	Enquired with management that they have obtained and reviewed SOC2 report for AWS	No Exceptions noted
<b>ADDITIONAL CRITERIA FOR AVAILABILITY</b>			
<b>A1.1</b>	<b>The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</b>		
	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements  Processing capacity on AWS is monitored by tools such as Newrelic on an ongoing basis.	Inspected a sample of capacity monitoring reports to verify that the capacity demand is documented and reviewed by management.  Inspected Newrelic report to determine that tool monitors and reports on uptime, outage and response time.	No Exceptions noted
	Processing capacity for cloud infrastructure for AWS is monitored by AWS Newrelic on an ongoing basis.	Inspected Newrelic settings to determine that alerts & thresholds have been setup for abnormal conditions such as low CPA utilization, network out , free storage etc.	No Exceptions noted
	Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.	Inspected redundancy measures for firewall and determined that there is a backup firewall in a high availability configuration	No Exceptions noted
<b>A1.2</b>	<b>The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</b>		

Ref No	Controls Implemented by EvaBot	Test Procedures	Test Results
	All customer data is on AWS and there is no critical data in EvaBot offices. Accordingly, A1.2 is not applicable.	Not applicable	Not Applicable
<b>A1.3</b>	<b>The entity tests recovery plan procedures supporting system recovery to meet its objectives.</b>		
	Disaster recovery and Business Continuity plans and procedures for various disruption scenarios are documented.	Inspected disaster recovery & Business Continuity plans to determine that these are documented.	No Exceptions noted
	Business continuity plans, including restoration of backups, are tested at least annually.	Inspected BCP/DR test report to determine that BCP plans have been tested.	No Exceptions noted
<b>ADDITIONAL CRITERIA FOR CONFIDENTIALITY</b>			
<b>C1.1</b>	<b>The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.</b>		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the retention policy to determine that the Company retains information as per the defined policies.	No Exceptions noted
<b>C1.2</b>	<b>The entity disposes of confidential information to meet the entity's objectives related to confidentiality.</b>		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the retention policy to determine that the Company destroys or disposes of confidential information as per the defined retention policies.	No Exceptions noted

## **SECTION 5**

**OTHER INFORMATION PROVIDED BY EVABOT**

## 5. Other Information Provided by EvaBot

The information provided in this section is provided for informational purposes only by EvaBot, Inc. Independent Auditor has performed no audit procedures in this section.

### **Disaster and Recovery Services**

The AICPA has published guidance indicating that business continuity planning, which includes disaster recovery, is a concept that addresses how an organization mitigates future risks as opposed to actual controls that provide user auditors with a level of comfort surrounding the processing of transactions. As a result, a service organization should not include in its description of controls any specific control procedures that address disaster recovery planning. Therefore, EvaBot, Inc's disaster recovery plan descriptions of control procedures are presented in this section.

In addition to the physical controls, EvaBot, Inc has implemented to safeguard against an interruption of service, EvaBot, Inc has developed a number of procedures that provide for the continuity of operations in the event of an extended interruption of service at its data center. In the event of an extended interruption of service, EvaBot, Inc will utilize backup site maintained at AWS.

The disaster recovery plan defines the roles and responsibilities and identifies the critical IT application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on a business impact analysis.