# System and Organization Controls (SOC) for Service Organizations

# SOC 3

For The

Conversational Email Platform

A Report on 6sense Insights, Inc.'s
System and Controls Relevant to Security

July 1, 2023, to November 30, 2024

Report of Independent Service Auditors issued by AssurancePoint, LLC

# TABLE OF CONTENTS

# SECTION I

## INDEPENDENT SERVICE AUDITOR'S REPORT

# Independent Service Auditor's Report

To Management of 6sense Insights, Inc.:

*Scope*

We have examined 6sense Insights, Inc.'s ("6sense" accompanying assertion included in Section 2 of this report that the controls within 6sense's Conversational Email Platform were effective throughout the period July 1, 2023, to, November 30, 2024, to provide reasonable assurance that 6sense's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

*Service Organization's Responsibilities*

6sense 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 6sense's service commitments and system requirements were achieved. 6sense has provided the accompanying assertion, in Section 2, ("Management's Assertion") about the effectiveness of controls within the system. When preparing its assertion, 6sense, is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls stated within the system.

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve 6sense's service commitments and system requirements based on the applicable trust services criteria;
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve 6sense's service commitments and system requirements based on the applicable trust services criteria;

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

*Inherent Limitations*

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

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

*Opinion*

In our opinion, management's assertion that the controls within 6sense's Conversational Email Platform were effective throughout the period July 1, 2023, to, November 30, 2024, to provide reasonable assurance that 6sense's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

AssurancePoint, LLC

Atlanta, Georgia
December 17, 2024

# SECTION 2

## MANAGEMENT'S ASSERTION

# Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within 6sense's Conversational Email Platform throughout the period July 1, 2023, to, November 30, 2024, to provide reasonable assurance that 6sense's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2023, to, November 30, 2024, to provide reasonable assurance that 6sense's service commitments and system requirements were achieved based on the applicable trust services criteria. 6sense's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2023, to, November 30, 2024, to provide reasonable assurance that 6sense's service commitments and system requirements were achieved based on the applicable trust services criteria.

# SECTION 3

## DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

# Overview of Operations

### Company Background

6sense Insights, Inc., herein referred to as 6sense, was founded in 2013 and has offices in San Francisco, New York, London, Pune, Bengaluru, and Austin. 6sense has financial backing from Insight Partners, Venrock, Industry Ventures, D1 Capital Partners, Sapphire Ventures, and Tiger Global with Series E funding in 2022.

6Sense is on a mission to revolutionize the way Business-to-Business (B2B) organizations create revenue by predicting customers most likely to buy and recommending the best course of action to engage anonymous buying teams.

6sense's Conversational Email Platform, commonly referred to as CE, was founded in 2016 by Saleswhale and acquired by 6sense in January 2022.

### Description of Services Provided

The 6sense Conversational Email Platform helps revenue teams automate lead conversion. The platform uses Artificial Intelligence (AI) to help marketing operations teams convert marketing qualified accounts into sales meetings at scale. The core of the Conversational Email Platform is an AI Lead Qualification Engine that engages leads in two-way email conversations and then qualifies and categorizes the "sales-ready" leads based on their replies, before sending them to the sales teams to schedule meetings.

# Components of the System

### System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

### Infrastructure and Software

Conversational Email is a software-as-a-service (SaaS) cloud-based system as part of the broader 6sense SaaS Platform ecosystem (refer also to the 6sense SaaS Platform SOC 2 Type 2 Report available on the 6sense trust center for further information). The primary components of the system are built on top of Amazon Web Services (AWS), using the following services.

| Primary Infrastructure | |
|---|---|
| **System/Software** | **Business Function Description** |
| Amazon Virtual Private Cloud (VPC) | Provides an isolated networking environment for private communication between services. |
| Elastic Container Service (ECS) | Scalable container orchestration service provided by AWS for deploying and managing Docker containers. |
| Docker | Allows the organization to create, deploy, and run applications in isolated, lightweight containers. |
| Relational Database Service (RDS) | Managed cloud database service provided by AWS for the setup, operation, and scaling of relational databases. |

| Primary Infrastructure | |
|---|---|
| **System/Software** | **Business Function Description** |
| S3 Buckets | Scalable and secure cloud storage containers provided by AWS for storing and retrieving data. |

Additionally, the following secondary systems and software are used to support the delivery of the SaaS service:

| Secondary Systems and Software | |
|---|---|
| **System/Software** | **Business Function Description** |
| GitHub | Change management and version control system |
| Dependabot | Detects and suggests updates for outdated dependencies in code repositories. |
| Datadog | Monitoring and analytics platform that provides real-time visibility into the performance of applications, infrastructure, and cloud environments |
| Jira | Project management and issue tracking tool that helps teams plan, track, and manage their work as well as track and respond to security events and incidents. |
| Slack | Cloud-based instant messaging and collaboration platform for teams to communicate and work together. |
| Kandji | Mobile device management (MDM) tool that enables the organization to remotely configure, monitor, and secure their mobile devices |

**People**

Personnel involved in the operation and use of the system are:

- 6sense Insights Singapore, Pte. Ltd Board of Directors – responsible for the overall financial, operational, and objectives of Conversational Email. Also responsible for the overall legal compliance of the business, including security functions and contractual commitments (e.g., with customers, vendors, contractors, employees, etc.).
- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- People Team – responsible for formulating HR policies, practices, and processes, prioritizing essential HR department functions such as talent acquisition, employee retention, compensation, employee benefits, performance management, employee relations, training, and development.
- Engineering Team – responsible for overseeing and leading development and data science operations to include building new features for the 6sense Conversational Email SaaS platform.
- Product Team – responsible for product management, including the formulation and implementation of the product roadmap.
- Infrastructure Team – Responsible for the availability, reliability, performance, and scalability of the 6sense Conversational Email SaaS platform.

**Data**

The system receives customer data, including content and leads, through an API integration with the customer's CRM instance. Alternatively, the customer can directly upload the data themselves. The customer provides pre-defined email templates to the Conversational Email Platform, and in turn, the Conversational Email Platform personalizes these emails. The customized emails are then sent back to the customer's email system. From there, the customer can send these personalized emails to their leads.

As the customer sends out emails, any responses from the leads are captured and integrated back into the system. These lead replies, along with other performance metrics and results, are made available to both the customer user and internal operators for analysis and monitoring.

**Procedures**

*Logical Access Infrastructure, Software, and Architecture*

The company maintains a formal inventory of production system assets, which provides an overview of the infrastructure and helps identify potential vulnerabilities. To access the production systems, the company mandates authentication using unique usernames and passwords or authorized SSH keys, ensuring that only authorized personnel can interact with the systems. Furthermore, passwords for in-scope system components must comply with the company's policy, which emphasizes strong and secure password practices.

An additional layer of security is implemented through Multi-Factor Authentication (MFA), which is required for the company's production system infrastructure management console and application code version control tool. Role-based access privileges are granted through predefined user access groups. By following this approach, the company ensures that individuals have access only to the resources necessary for their specific roles, reducing the attack surface. Customers are required to access the application using a unique username and password and have the option to enable single sign-on (SSO).

To protect customer data, the company's network is segmented to prevent unauthorized access. This segmentation isolates sensitive information, limiting the potential impact of security incidents. Privileged access to production systems is restricted to authorized users with a legitimate business need, reducing the likelihood of unauthorized actions that could jeopardize the system's security.

*Access Authorization and Access Revocation*

The company's access control policy outlines the procedures for various access control functions, including adding new users, modifying existing users, and removing access for individuals who no longer require it. When a new hire joins the company, a standard user onboarding ticket is initiated, which encompasses the provisioning of user access permissions tailored to their specific job role and responsibilities.

To help ensure that user access aligns with their job roles and functions, or if a specific access request is needed, employees must submit a documented access request form that requires managerial approval before access is granted. This ensures a thorough review and approval process for granting access.

To maintain the security of in-scope system components, the company conducts access reviews at least once a year. These reviews assess the appropriateness of access and help identify any areas where access needs to be restricted or modified. Any necessary changes resulting from these reviews are tracked until completion.

Moreover, the company utilizes termination workflows to ensure that access is promptly revoked for employees who are no longer with the company, minimizing the risk of unauthorized access after an individual leaves their role.

*Perimeter Security*

Firewalls are deployed and configured to block unauthorized access attempts, acting as a barrier against external threats. The company encrypts its datastores housing sensitive customer data at rest. Encryption ensures that even if unauthorized access is gained, the data remains unreadable, safeguarding it from potential breaches.

To maintain continuous network monitoring and detect potential security breaches early, the company utilizes an intrusion detection system, providing an additional layer of security to its network infrastructure.

*Data Transmissions*

Documented policies and procedures are in place which require the encryption of confidential or sensitive data sent over public networks. For data protection during transmission, the company employs secure data transmission protocols that encrypt confidential and sensitive data with TLS encryption when transmitted over public networks.

*Employee Workstation Anti-malware and Encryption*

Employee workstations are centrally managed through a Mobile Device Management (MDM) system, enabling the company to maintain control and security over these devices. Antivirus software is implemented on employee workstations, ensuring a proactive approach to detecting and mitigating potential threats before they can cause harm. Employee workstations are also configured with disk encryption, which serves as a safeguard against data theft or unauthorized access to critical information, including customer data.

*System Monitoring*

The company follows a defined process to help ensure robust information security practices are maintained throughout its environment. The first step involves deploying a standard container configuration to help ensure consistent system settings across the production environment. Vulnerability management and system monitoring policies are in place to establish clear requirements for handling vulnerabilities and continuously monitoring systems to detect potential security threats.

To facilitate control and compliance, the company employs a security and compliance application. This application continuously monitors control performance and gathers process control data, which is then translated into actionable information for personnel that aids in supporting internal control functions.

In line with maintaining a secure environment, the company utilizes log management tools. These tools help identify events that may have adverse effects on the company's security objectives. Both source code and container image repositories undergo continuous vulnerability scans. Identified critical and high-level vulnerabilities are tracked for remediation. Additionally, a third-party provider performs an annual external vulnerability scan. Upon identification of vulnerabilities, a remediation plan is developed, and changes are implemented in alignment with Service Level Agreements (SLAs).

*Incident Response*

The company follows a structured workflow for handling security incidents and ensuring business continuity. The company has established security incident response policies and procedures that are documented and communicated to authorized users across the organization. This ensures that relevant stakeholders are aware of the necessary steps to be taken in the event of a security incident.

When a security incident occurs, the company logs and tracks the incident, initiating the resolution process. The management takes charge of overseeing the response efforts, ensuring that the incident is effectively dealt with and mitigated according to the company's security incident response policy and procedures. Additionally, affected or relevant parties are kept informed and updated throughout the incident management process.

To maintain the effectiveness of their incident response plan, the company conducts periodic testing of the plan at least once a year. This allows them to identify any potential gaps or areas of improvement, enabling them to refine their response procedures and ensure that their incident response capabilities remain up-to-date and effective.

Furthermore, the company has a documented BC/DR plan in place. This plan outlines strategies and protocols to help ensure the organization's critical operations can be maintained or quickly resumed in the face of disruptive incidents. To verify the plan's readiness and effectiveness, the company conducts an annual test of their BC/DR plan.

*Change Management*

The company's development process follows an established Software Development Life Cycle (SDLC) methodology that governs the entire lifecycle of information systems and related technology requirements. This methodology encompasses development, acquisition, implementation, change, and maintenance procedures.

To maintain version control and ensure transparency throughout the change management process, the company utilizes version control software. This software enables development personnel to track and document changes made to the codebase, promoting accountability, and facilitating effective collaboration among development teams. The company has implemented a secondary approval process for pull requests. Before any changes can be merged into the master branch, they must undergo a thorough review and obtain approval from designated personnel, ensuring code quality and security. Additionally, testing and vulnerability scanning are carried out on code changes before they are merged into the master branch. This proactive approach helps identify and address potential vulnerabilities, reducing the risk of security breaches.

To help ensure a secure transition from development to production, changes to system infrastructure and applications are developed and tested in development and test environments separate from the production environment. This approach mitigates the chances of introducing errors or issues into the production environment. Access to deploy changes into production is restricted to authorized personnel, emphasizing the importance of access control, and minimizing the possibility of unauthorized changes or malicious activities.

To keep engineering personnel informed about production deployments, a designated Slack channel is used for notifications. This ensures that the relevant team members are aware of changes and can respond promptly if any issues arise.

Finally, to maintain a secure infrastructure, routine maintenance includes patching the infrastructure supporting the service. This practice helps ensure that containers supporting the service remain hardened against potential security threats, safeguarding the overall system integrity.

## Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable trust services criteria that are intended to be met by controls at AWS, alone or in combination with controls at 6sense, and the types of controls expected to be implemented at AWS to achieve 6sense's service commitments and system requirements based on the applicable trust services criteria.

| Control Activity Expected to be Implemented by AWS | Applicable Trust Services Criteria |
|---|---|
| AWS is responsible for restricting physical access to data centers housing hardware and physical infrastructure in which production data resides. | CC6.4 |
| AWS is responsible for diminishing the ability to read and recover data and software from physical assets prior to discontinuing logical and physical protections over those assets. | CC6.5 |

## Complementary User Entity Controls

6sense's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

# SECTION 4

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

## Principal Service Commitments and System Requirements

The company designs its processes and procedures related to the Conversational Email Platform to meet the objectives management has established for its services. Those objectives are based on the service commitments that the company makes to user entities; the laws and regulations that govern the provision of the services; and the financial, operational, and compliance goals management has established for the services.

Management has formally established commitments to user entities, including commitments over the security of information processed by its system. These commitments are foundational to the objectives of the organization and are supported by relevant system requirements. The principal service commitments and system requirements related to the Conversational Email Platform are those commitments and system requirements that are applicable to the broad base of users and include the following:

*Security Commitments*

- Maintains a written security program that includes administrative, technical, and physical safeguards reasonably designed to protect customer data.
- Business continuity and disaster recovery (BC/DR) plan in place to manage significant disruptions to operations and infrastructure.
- Access controls in place designed to maintain the security of customer data.
- Collect and record log information and maintain system logs based on residual risk and commensurate with industry expected operating practices.
- Asset management program in place that appropriately classifies and facilitates control and management of hardware and software assets throughout their lifecycle.
- Documented risk assessment and management process to identify, rate and treat identified risks to the organization.
- Conduct background checks for its employees that will have access to customer data.
- Require employees to complete security training.
- Appropriate network perimeter defense solutions in place to monitor, detect, and prevent malicious network activity and restrict access to authorized users and services.
- Software development lifecycle ("SDLC") methodology in place that governs the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components as applicable.
- Follow documented change management policies and procedures for requesting, testing, and approving application, infrastructure, and product related changes.
- Threat and vulnerability management program that includes on-going monitoring for vulnerabilities.
- Assess the risks associated with any new and existing service providers that have access to customer data.
- Notify customer via email without undue delay upon confirmation of a customer data security incident, reasonably cooperate with customer with respect to any such customer data security incident, and take appropriate action as seems necessary to mitigate risks or damages associated with the customer data security incident to protect customer data from further compromise.

*System Requirements*

- Continuous Control Monitoring
- Access Management
- Employee Lifecycle Management
- Endpoint Device Management
- Business Continuity and Disaster Recovery

- Change Management
- Data Classification
- Software Development Lifecycle (SDLC)
- Incident Response
- Logging and Monitoring
- External Penetration Testing
- Operational Risk Management
- User Access Reviews
- Third Party Risk Management
- Vulnerability Management

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.