



SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON
MANAGEMENT'S ASSERTION RELATED TO ITS

Smartcat AI Translation Platform

Relevant to Security

For the period April 15, 2025 to July 15, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:



Sensiba

Table of Contents

1. Independent Service Auditors' Report.....	1
Scope	1
Service Organization's Responsibilities	1
Service Auditors' Responsibilities	1
Inherent Limitations	2
Opinion	2
2. Assertion of Smartcat Management	3
3. Description of Smartcat's AI Translation Platform.....	4
Company Background	4
Services Provided.....	4
Principal Service Commitments and System Requirements.....	4
Components of the System	5

1. Independent Service Auditors' Report

To the Management of Smartcat Platform Inc. (Smartcat)

Scope

We have examined Smartcat's accompanying assertion titled "Assertion of Smartcat Management" (assertion) that the controls within Smartcat's AI Translation Platform (system) were effective throughout the period April 15, 2025 to July 15, 2025, to provide reasonable assurance that Smartcat'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Service Organization's Responsibilities

Smartcat 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 Smartcat's service commitments and system requirements were achieved. Smartcat has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Smartcat is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether 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 AICPA. 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.

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 Smartcat’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 Smartcat’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.

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

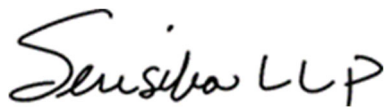
Inherent Limitations

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 were 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 Smartcat’s AI Translation Platform were effective throughout the period April 15, 2025 to July 15, 2025, to provide reasonable assurance that Smartcat’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California

September 2, 2025

2. Assertion of Smartcat Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Smartcat Platform Inc. (Smartcat) AI Translation Platform (system) throughout the period April 15, 2025 to July 15, 2025, to provide reasonable assurance that Smartcat's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Smartcat's AI Translation Platform," (description) 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 April 15, 2025 to July 15, 2025, to provide reasonable assurance that Smartcat'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA, *Trust Services Criteria*.

Smartcat'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 the accompanying system description.

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 April 15, 2025 to July 15, 2025, to provide reasonable assurance that Smartcat's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Smartcat Management

September 2, 2025

3. Description of Smartcat's AI Translation Platform

Company Background

Founded in 2016, Smartcat is an AI-powered language and translation platform designed for global enterprises. It offers a suite of tools for content creation, translation, and localization, aiming to streamline global content workflows through automation and AI-human collaboration. The company emphasizes speed, scale, and brand control in its solutions, serving over 1,000 clients, including a significant portion of the Fortune 1000.

Services Provided

Smartcat is an AI-powered language platform designed to help global companies manage and automate their content creation, translation, and localization processes. It offers tools for producing content in multiple languages, translating various formats such as documents, websites, software, and videos, and streamlining workflows with AI-powered agents. Additionally, Smartcat provides access to a marketplace of linguists and editors for complex or high-stakes content.

Smartcat delivers SaaS (Software as a Service) cloud services through a cloud-based platform for translation and localization workflows that end-users access via a web browser, eliminating the need to manage underlying infrastructure. While it uses cloud infrastructure, its primary focus is on providing a comprehensive software solution for translation management within the SaaS model.

Smartcat operates globally, with employees across multiple continents and a large customer base in many countries.

Principal Service Commitments and System Requirements

Smartcat Platform Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Smartcat Platform Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Smartcat Platform Inc. has established for the services. The system services are subject to the Security commitments established internally for its services.

Security commitments

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system

- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up-time availability of production systems

Components of the System

Infrastructure

Smartcat Platform Inc. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Various Services, including VPC, Elastic IP, IAM, Lambda, Application Load Balancer	Cloud Infrastructure
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload, and download
MongoDB	AWS	Contains PII and client data

Software

Primary Infrastructure	
Software	Purpose
HiBob	User and organization information of Smartcat employees and contractors
HubSpot	Information of Smartcat clients
GitLab	Source code and company intellectual property
Notion	Operational, support procedures, and system documentation
YouTrack	Task management system utilized to centrally track, maintain, and manage internal requests (e.g., access requests) and change management activities
Smartcat VPN	Access to critical services

People

The company employs dedicated team members to handle major product functions, including operations, and support. The Infrastructure and DevOps Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Smartcat Platform Inc. has a staff of approximately 250 organized in the following functional areas:

Executive Leadership: Top Management is Individuals who are Responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

Account Management: Responsible for building and maintaining strong relationships with existing clients. They ensure client satisfaction, manage renewals, and identify opportunities for account expansion.

Product Management: Focuses on the strategy, development, and launch of the company's products. They define product roadmaps, gather user feedback, and collaborate with engineering to bring new features to life.

Sales Team: Drives revenue by acquiring new customers and closing deals. They identify potential clients, present the value of Smartcat's solutions, and negotiate contracts to meet company targets.

Finance: Manages the company's monetary resources. They handle budgeting, financial reporting, payroll, and forecasting to ensure the company's fiscal health and compliance.

Marketing: Promotes the company's brand and generates leads. They create campaigns, manage public relations, and develop content to attract potential customers and increase brand awareness.

Engineering and Development: Builds and maintains the technology that powers Smartcat. They design, code, and test software to ensure the platform is robust, scalable, and innovative.

Human Resources: Manages all aspects related to the company's employees. They handle recruitment, employee relations, payroll, benefits, and ensure a positive and productive work environment.

Information Security: Oversees the implementation of information security controls for infrastructure and IT processes; responsible for the design, development, implementation, operation, maintenance, and monitoring of cybersecurity controls; communicates information security risks to executive leadership.

Data

Data as defined by Smartcat Platform Inc., constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Smartcat Platform Inc.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Smartcat Platform Inc..	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Smartcat Platform Inc.. Smartcat Platform Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Smartcat Platform Inc. to operate the business. Smartcat Platform Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Smartcat Platform Inc. has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Processes, Policies and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Smartcat uses Amazon Web Services (AWS) for cloud computing and storage. Amazon manages access to the network, system management, and storage devices hosting Smartcat data.

Amazon handles the physical security and environmental controls at data center facilities hosting Smartcat systems. Therefore, those facilities are outside the scope of physical security and environmental controls.

Amazon is responsible for securely deleting data and properly disposing of equipment used to support Smartcat client operations.

Logical Access

Smartcat Platform Inc. provides employees and contractors with access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reproducible user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

The Information Security team and DevOps team are responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Smartcat Platform Inc.'s policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, the Information Security team and DevOps team are responsible for deprovisioning access to all in-scope systems within 3 days of that employee's termination.

Computer Operations – Backups

Customer data is backed up and monitored by the DevOps team for completion and exceptions. If there is an exception, the DevOps team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with logical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations – Availability

Smartcat Platform Inc. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Smartcat Platform Inc. internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

Smartcat Platform Inc. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Control

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

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

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

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Zone-redundant resources are distributed across multiple availability zones. If a primary system fails, the redundant infrastructure services are designed to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing encompasses network and application layer testing, as well as the evaluation of controls and processes surrounding networks and applications, conducted both from the outside (external testing) and from within the network.

Automatic vulnerability scanning is performed continuously following the Vulnerability Management policy. Vulnerability scanners are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the processes, systems, and software managed by Smartcat to deliver its Services. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.

Control Environment

Integrity and Ethical Values

The effectiveness of controls is directly linked to the integrity and ethical values of the individuals who design, administer, and monitor them. Integrity and ethical values are fundamental components of Smartcat Platform Inc.'s control environment, influencing the design, administration, and oversight of other elements.

Integrity and ethical behavior stem from Smartcat Platform Inc.'s moral and behavioral standards, as well as how these standards are communicated and reinforced in practice. This includes management's efforts to eliminate or reduce incentives and temptations that might lead employees to engage in dishonest, illegal, or unethical behavior. Additionally, it encompasses the communication of the company's values and behavioral standards to employees through policy statements and codes of conduct, as well as through leading by example.

The service organization has implemented specific control activities in this area, which are outlined below:

- Clearly documented organizational policy statements and codes of conduct communicate the entity's values and behavioral standards to all personnel.
- Policies and procedures require employees to sign an acknowledgment form confirming that they have received access to the employee manual and understand their responsibility to adhere to the policies and guidelines within it.
- A confidentiality statement is included in the employee handbook, which requires employees to agree not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks are conducted on employees as part of the hiring process.

Commitment to Competence

Smartcat Platform Inc.'s management defines competence as the knowledge and skills required to effectively perform the tasks associated with employees' roles and responsibilities. The management is committed to assessing the competence levels needed for each position and understanding how these levels correspond to the necessary skills and knowledge.

The service organization has implemented specific control activities in this area, which are outlined below:

- Management has assessed the required competence levels for different jobs and documented the necessary skills and knowledge for each position.
- Additionally, training is offered to ensure that personnel in certain roles maintain their skill levels.

Management's Philosophy and Operating Style

The management team at Smartcat Platform Inc. faces a challenge in balancing two competing interests: they must continue to grow and innovate in a rapidly changing technology landscape while also being responsible and careful stewards of the sensitive data and workflows that customers trust us with.

The management team meets regularly to stay updated on technological changes that affect how Smartcat Platform Inc. assists customers in building data workflows. They also discuss new security technologies that can help protect these workflows, along with any regulatory changes that may require adjustments to the software for legal compliance. Additionally, the management team reviews major planned changes to the business to ensure that these changes align with our core product offerings and our responsibilities to both new and existing customers.

The service organization has implemented several specific control activities in this area, which are outlined below:

- Management receives periodic briefings on regulatory and industry changes that impact the services provided.
- Executive management meetings are convened to discuss significant initiatives and issues affecting the business.

Organizational Structure and Assignment of Authority and Responsibility

Smartcat Platform Inc. has developed an organizational structure that serves as a framework for planning, executing, controlling, and monitoring activities to achieve its overall objectives. Management recognizes the importance of defining key areas of authority and responsibility in establishing an effective organizational structure. This structure has been tailored to meet the company's specific needs, taking into account its size and the nature of its activities.

Smartcat Platform Inc. outlines its assignment of authority and responsibility through several key activities. This includes defining how authority and responsibility for operational tasks are assigned, as well as establishing reporting relationships and authorization hierarchies.

Additionally, the company implements policies that promote appropriate business practices and ensure that key personnel possess the necessary knowledge and experience. Resources are also allocated to support the execution of these duties.

Smartcat highlights the need for communication and policies that help employees understand the company's objectives. Employees are encouraged to see how their individual actions contribute to these goals and recognize the accountability tied to their roles.

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

- Organizational charts are used to clarify key areas of authority and responsibility.
- These organizational charts are communicated to employees and updated as necessary.

Human Resource Policies and Practices

Smartcat Platform Inc. owes its success to a strong foundation of business ethics, characterized by high levels of efficiency, integrity, and ethical standards. This success is demonstrated by the company's proven ability to hire and retain top-quality personnel, ensuring that the organization operates at maximum efficiency. The human resources policies and practices at Smartcat Platform Inc. encompass various aspects, including employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary procedures.

The service organization has implemented the following specific control activities:

- New employees must sign acknowledgment forms for the employee handbook and a confidentiality agreement on their first day of employment, following new hire orientation.
- Annual evaluations are conducted for each employee.
- There are documented termination procedures, including a checklist, to guide the employee termination process.

Risk Assessment Process

Smartcat Platform Inc. has a risk assessment process in place to identify and manage risks that could impact our ability to provide reliable and secure services to our customers. To support this process, we maintain a risk register that tracks all systems and procedures posing potential risks to the company's objectives. We evaluate risks based on their likelihood and impact, and management develops action plans for those risks that score highly in both areas. The risk register is reviewed and updated annually, and the identified tasks are integrated into our regular product development cycle to ensure they are addressed in a predictable and iterative manner.

Integration with risk assessment

The environment in which the Smartcat Platform Inc. system operates, along with its commitments, agreements, and responsibilities, presents certain risks that may prevent criteria from being met. Smartcat Platform Inc. tackles these risks by implementing well-designed controls to provide reasonable assurance that the criteria are satisfied. Since every system and its operational environment are unique, the combination of risks associated with meeting the criteria and the corresponding controls will also be distinctive. As part of the system's design and operation, Smartcat Platform Inc.'s management identifies specific risks that may hinder meeting the criteria and determines the necessary controls to address those risks.

Information and Communications Systems

Information and communication are essential components of Smartcat Platform Inc.'s internal control system. This process involves identifying, capturing, and exchanging information in a timely manner to effectively conduct, manage, and control the organization's operations.

Smartcat Platform Inc. utilizes various channels to share information internally with management, employees, contractors, and customers. The primary communication methods include chat systems and email for both internal and external communication.

Structured data is shared through SaaS applications and project management tools. Additionally, the company conducts in-person and video "all hands" meetings to convey company priorities and goals from management to all employees.

Monitoring Controls

Management oversees controls to ensure they function as intended and are adjusted as conditions evolve. Smartcat Platform Inc.'s management conducts monitoring activities to continuously evaluate the quality of internal controls over time. When deviations from company policies and procedures occur, necessary corrective actions are taken. Additionally, employee activities and compliance with company policies are monitored. This process is carried out through ongoing monitoring activities, separate evaluations, or a combination of both.

On-going monitoring

Smartcat Platform Inc. conducts regular quality assurance monitoring, and additional training is provided based on the results of these monitoring procedures. These monitoring activities are utilized to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management plays a crucial role in Smartcat Platform Inc.'s operations by identifying significant variances from expectations related to internal controls. Upper management evaluates the facts and circumstances surrounding any suspected control breakdowns. Decisions regarding how to address any weaknesses in controls depend on whether the incident was isolated or necessitates changes to the company's procedures or personnel. The objective of this process is to ensure legal compliance and to enhance the performance of Smartcat Platform Inc.'s personnel.

Reporting deficiencies

Our internal risk management tracking tool is used to document and monitor the results of ongoing monitoring procedures. We maintain escalation procedures to respond to and inform management of any identified risks. Detailed instructions for escalation are provided to employees in the company policy documents. Risks that receive a high rating are addressed immediately. If corrective actions are necessary, they are documented and tracked in the internal tracking tool. Additionally, we hold annual risk meetings for management to review reported deficiencies and the actions taken to correct them.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Smartcat's AI Translation Platform.

Subservice Organizations

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

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

Security Category	
Criteria	Controls expected to be in place
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	

Security Category	
Criteria	Controls expected to be in place
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Smartcat management, along with the subservice organization, define 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, Smartcat performs monitoring of the subservice organization controls, including the following procedures

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

- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

Smartcat's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Smartcat's services to be solely achieved by Smartcat's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Smartcat's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

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