Infrastructure Change Assessment

Version 1.0
Last Updated: January, 2025

Contents

Scope

The purpose of the document is to highlight the compliance, security and technical evaluation carried out before the planned migration of services from the Heroku platform into the Amazon Web Services (“AWS”) infrastructure. The assessment was designed to appraise security, compliance, and performance requirements, assess and minimize risks that could arise from this change.

Overview

This document summarizes the security and technical controls and the assessment performed by CloudSense in preparation for the upcoming infrastructure migration. The primary objective of this assessment was to ensure that the security and technical controls are robust and aligned with industry best practices, contractual and regulatory requirements, as well as organizational standards, before the migration takes place.

The assessment evaluated critical areas such as network security, encryption, data protection, access control, authentication, performance, as well as incident response, sub-processors, and service continuity to identify potential vulnerabilities and risks. Our methodology involved a combination of technical reviews, risk assessments and operational reviews. Compliance with relevant regulations, including the GDPR, was a key consideration in the evaluation process.

Security Controls for Data Protection

Encryption implementation. Services are designed to provide data security and integrity. Data storage components in the new environment will have industry-standard encryption levels applied which are as strong as the current encryption solutions or stronger.

Encryption at rest. There is no change in encryption status for data storage that is not in scope for the migration.

Encryption in transit. Communication between customers or third-party systems and the Cloudsense Solution will be done via encrypted channels like HTTPS/SSL.

Network security and segmentation. The Cloudsense Solution internal server-to-server communication uses SSL and network isolation. Customer instances will continue to reside within customers' organization structure in platforms like Salesforce.

Authentication methods. We have established the requirements for ensuring authorized use of computing resources via proper user identification and password authentication.
Administrative access to the components deployed in AWS is only allowed through VPN with Two-Factor Authentication. AWS Identity and Access Management (IAM) is used to define individual users and privileged accounts with permissions across AWS resources.

Access controls. We have established mechanisms for controlled access to computing resources. Based on business process controls and data classification policies, the level of access is determined for a user, a process, or a system.
Administrative access to the AWS system components is granted with manager approval and based on the least privilege principle.

Physical security controls. Data centers located at AWS facilities and physical access is strongly controlled by AWS according to its own Information security policy and physical access controls. Such access is limited to AWS employees and authorized personnel only. Physical access to server rooms is closely monitored with CCTV, and access to data centers is controlled using surveillance systems. Electronic intrusion detection systems are in place to monitor and alert security personnel to any security incidents.

Additional Data Protection Measures

Server hardening. New system components are deployed using server hardening protocols that include removing unnecessary services and network protocols, limiting authorized users who can configure the system, carefully setting access controls by using a deny-by-default approach, addressing potential vulnerabilities.

Anti-intrusion. Our organization evaluates the intrusion risk to systems and takes additional measures to mitigate such risk, where deemed necessary.

Risk assessment. Our teams have performed a risk assessment of the activities planned and changes expected with the migration. Mitigating actions were taken or planned for key findings

to ensure that known risks are managed proactively and as early as possible.
Participation of our customers with endpoint configuration changes and validation testing is critical in ensuring a smooth transition.

Maintaining and Improving Security Controls

Change management. Our teams follow established mechanisms for change management and control to mitigate risks associated with changes to information systems covered. These changes follow defined planning, evaluation, review and approval procedures.

Monitoring and logging. Systems will continue to be monitored and logs will be maintained as a comprehensive strategy for managing the systems in the new environment. These will be integrated with a robust internal notification system to alert administrators of events that may require attention, provide real-time awareness and help with troubleshooting, compliance, and future improvements.

Penetration/vulnerability testing. We use industry-standard tools to carry out network vulnerability scans and perform web application scans based on the Open Web Application Security Project (OWASP) Top 10. Such security testing is a key way to identify vulnerabilities, to ensure that the existing security precautions are effective and that security controls are configured properly.

Service Levels

Service continuity. We have established standards, processes, and controls for the timely recoverability of business critical data and information processing systems. Our Support channels will be open 24/7 to provide assistance during the migration period.

Rollback capabilities. During the transition we will maintain parallel systems operating with both the existing and the new infrastructure, to allow for a prompt fallback if needed.

Service availability. We will provide advance notice for the maintenance windows scheduled for the migration activities. Service monitoring systems will track performance metrics and system health throughout the migration process. System status is posted at: https://skyvera.statuspage.io/

Processing and performance capabilities. We do not foresee changes to key processing capabilities and performance metrics. Certain configuration changes (endpoint updates) are required to be done by customers on their end and are key to maintaining migration timelines. Our teams will provide guidance and will be available to provide support for these configuration changes.
Customer involvement with this migration is also required for testing and validation of the system in the new environment.

Security incident response. Our privacy and security incident response plan is designed to provide guidance to staff on how to report and address suspected security incidents. This plan outlines steps to be taken in order to investigate potential security breaches and includes performing a risk analysis to determine notification requirements, performing mitigation and remediation actions, conducting lessons learned sessions and determining preventive measures.

Key Sub-Processors and Processing Activities

Overseeing service providers. Our organization has implemented a third-party management program with the purpose of selecting service providers that are capable of maintaining appropriate safeguards for personal and other types of sensitive data. The privacy team works with legal counsel to develop and incorporate standard contractual protections applicable to third-party service providers, which require such providers to implement and maintain appropriate data security safeguards. In addition, these service providers are subject to periodic risk assessment.
Below are the key sub-processors and processing activities they are performing:

- **Amazon Web Services** has been the hosting provider for the Heroku platform and its data storage components and will remain so with this transition. Services previously used through the Heroku platform will now be used directly in AWS.
  AWS maintains best-in-class security and provides the benefits of increased flexibility, limitless scalability, improved monitoring and notification, and a series of industry recognized security certifications including ISO 27001, and SOC1 and SOC2, among others.
  Name: Amazon Web Services, Inc.
  Address: 410 Terry Ave. N., Seattle, WA 98109, USA
- **Salesforce** will continue to be a key sub-processor and there are no changes planned with regards to the integration with the CloudSense Solution or any Salesforce add-on

components.

Name: Salesforce, Inc.
Address: Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 94105, USA

Our organization group maintains Data Protection Agreements in place with AWS and Salesforce.
No new sub-processors are expected to be onboarded as part of this migration.

Data Processing & Geographic Locations

Data centers location. The location regions of the data storages will be maintained with the infrastructure migration. Data stored via Heroku components and add-ons will not be transferred outside of the regions previously used. Systems hosting will be maintained in:

- AWS Asia Pacific (Sydney);
- AWS US East (N. Virginia);
- AWS Europe (Ireland).

Cross-border transfer controls. CloudSense has established safeguards for the international transfer of personal data in accordance with applicable data protection laws, such as the European Union's General Data Protection Regulation. CloudSense enters into Standard Contractual Clauses with customers as part of the Company's Global Privacy Addendum.

Data handling procedures. Our organization has established policies and procedures to handle data protection throughout the data lifecycle, including data collection, storage, processing, transfer, and deletion.
Old systems will be decommissioned promptly after the validation of a successful migration.
No changes are expected to the Application Programming Interface or User Interface features that allow adherence to Individual's Rights under applicable privacy regulations.

Compliance with data privacy and data protection requirements. This migration does not affect the organization's compliance with data privacy and data protection regulations like the General Data Protection Regulation, the UK Data Protection Act, the Australian Privacy Act, the California Consumer Privacy Act. CloudSense and affiliates used to deliver the services are committed to supporting customers in their efforts to comply with applicable data protection regulations.