System and Organization Controls (SOC) 3

Report on Halo Services Solution Ltd.'s Platform Relevant to Security Throughout the Period October 1, 2024, to September 30, 2025



INSIGHT ASSURANCE

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT 1

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION 2

SECTION 2: «COMPANY LEGAL NAME» «COMPANY LEGAL NAME POSSESSIVE» MANAGEMENT ASSERTION 4

«COMPANY LEGAL NAME» «COMPANY LEGAL NAME POSSESSIVE» MANAGEMENT ASSERTION **ERROR! BOOKMARK NOT DEFINED.**

ATTACHMENT A: DESCRIPTION OF THE SYSTEM BOUNDARIES 6

«COMPANY LEGAL NAME» «COMPANY LEGAL NAME POSSESSIVE» DESCRIPTION OF THE BOUNDARIES OF THE «SYSTEM NAME» **ERROR! BOOKMARK NOT DEFINED.**

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 10

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 11

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION

To: Halo Services Solution Ltd.**Scope**

We have examined Halo Services Solution Ltd.'s ("Halo") accompanying assertion titled "Halo Services Solution Ltd.'s Management Assertion" (assertion) that the controls within the Platform (system) were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Halo'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

Halo 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 Halo's service commitments and system requirements were achieved. Halo has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Halo 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 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 Halo'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 Halo'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 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 the Platform were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Halo's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
November 28, 2025

SECTION 2:
HALO SERVICES SOLUTION LTD.'S MANAGEMENT ASSERTION



HALO SERVICES SOLUTION LTD.'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Halo Services Solution Ltd.'s ("Halo") Platform throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Halo'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*. Our description of the boundaries of the system is presented in Attachment A 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 October 1, 2024, to September 30, 2025, to provide reasonable assurance that Halo Services Solution Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria. Halo Services Solution Ltd.'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 Attachment B.

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 October 1, 2024, to September 30, 2025, to provide reasonable assurance that Halo Services Solution Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Halo Services Solution Ltd.
November 28, 2025

ATTACHMENT A:
DESCRIPTION OF THE SYSTEM BOUNDARIES

ATTACHMENT A

HALO SERVICES SOLUTION LTD.'S DESCRIPTION OF THE BOUNDARIES OF THE PLATFORM

SERVICES PROVIDED

The Halo Platform provides an all-included, highly customizable service packaged into 3 products for its distinct use cases & target markets: HaloPSA, HaloITSM, and HaloCRM. The Halo Platform focuses on providing an ITIL aligned service that standardizes processes, delivers analytics, and matches IT delivery to the needs of the business through digital workflows and automations.

INFRASTRUCTURE

Halo 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.

The in-scope infrastructure components are shown in the table below:

Primary Infrastructure		
Component	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	AWS	Scalable cloud computing.
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.

SOFTWARE

Halo is responsible for managing the development and operation of the Halo software solutions including infrastructure components such as servers, databases, and storage systems.

The in-scope Halo software components are shown in the table provided below:

Primary Software	
System/Application	**Purpose**
GuardDuty	Security application used for automated intrusion detection (IDS)
Redis	Used to maintain cached data

PEOPLE

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering 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 in their specific tasks and on the ways to keep the company and its data secure.

Halo has 220 staff members organized in the following functional areas:

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

- *Managing Director*: Oversight of cyber risk and organization direction concerning information security, privacy, and compliance.
- *Operation Manager/HR Manager*: Ensure a qualified and competent workforce by overseeing hiring, training, and performance evaluations; enforce security, confidentiality, and regulatory compliance through employee and contractor management, vendor oversight, and customer contract reviews.
- *Chief Technical Officer & Head of Infrastructure*: Lead the design, implementation, and oversight of security controls and risk management for production infrastructure, cloud hosting, and software development, ensuring alignment with company goals and regulatory standards while managing identity, access, and policy development processes.
- *Security Manager*: Oversee and manage the implementation and monitoring of information security tools and processes in customer environments, conduct IT risk assessments, maintain the risk register, and communicate security risks to leadership to ensure informed decision-making and risk mitigation.
- *Systems Administrator*: Design, implement, and maintain IT security controls, ensuring alignment with the Information Security Framework; managing device security, identity management, and access control for IT processes and infrastructure.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Product: Responsible for directing product direction, consultancy, implementation, and providing on-going support to clients; maximizing quality-of-life & customer retention.

Sales & Marketing: Responsible for company marketing and promotions across all platforms and the proceeding qualification and negotiation of prospective customers.

Accounting & Operations: Responsible for maintaining internal processes, tools, and systems to support the finance and business operations teams.

Legal, People & Partnerships: Responsible for legal, risk management, compliance, people administration, and partner relations.

DATA

Data as defined by Halo, 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 Halo:

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for Halo.	• 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 Halo. Halo must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Halo to operate the business. Halo 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, Halo 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.

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.

ATTACHMENT B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

Halo's Security commitments are communicated through the description of the platform as a whole, terms & conditions of the service provided with customers, support SLAs and event reports.

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.