SOC 2 Type 2 Report

Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)

FORESIGHT
PEOPLE BUILD FASTER WITH AI

June 2026

Shiff Hazenfratz & co.
RSM

Table of Contents

SECTION 1: MANAGEMENT ASSERTION

We have prepared the accompanying description of Foresight Service organization's (Foresight) hosted customer services system in the section entitled "Foresight Description of its Infrastructure Services System Throughout the Period January 1st, 2025, to December 31st, 2025", based on the criteria for a description of a service organization's system identified in paragraph 1.34 of the AICPA guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2 SM) (AICPA, *Description criteria*). The description is intended to provide users with information about the Infrastructure Services System in Foresight, particularly system controls that Foresight designed, implemented, and operated to meet the criteria for the security and availability principles (applicable trust services criteria) set forth in TSP section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids).

The description fairly presents the Infrastructure Services System throughout the period January 1st, 2025, to December 31st, 2025, based on the following description criteria:

The description contains the following information:

i. The types of services provided.

ii. The components of the system used to provide the services, as follows:
   (1) Infrastructure. The physical and hardware components of Foresight system (facilities, equipment, and networks)
   (2) Software. The programs and operating software of Foresight system (systems, applications, and utilities)
   (3) People. The personnel involved in the operation and use of Foresight system (developers, operators, users, and managers)
   (4) Procedures. The automated and manual procedures involved in the operation of Foresight system
   (5) Data. The information used and supported by Foresight system (transaction streams, files, databases, and tables)

iii. The Boundaries aspects of Foresight system covered by the description.

iv. How Foresight system captures and addresses significant events and conditions.

v. The process is used to prepare and deliver reports and other information to user entities or other parties.

vi. Any applicable trust services criteria that are not addressed by a control in the Foresight and the reasons therefore.

vii. Other aspects of Foresight's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

viii. Relevant details of changes to Foresight's system during the period covered by the description.

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

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

a. The controls stated in the description were suitably designed throughout the period January 1, 2025, to December 31, 2025, to meet the applicable trust services criteria and the CCM criteria; and

b. The controls stated in the description operated effectively throughout the period January 1, 2025, to December 31, 2025, to meet the applicable trust services criteria and the CCM criteria.

SECTION 2: INDEPENDENT SERVICE AUDITOR'S REPORT

Scope

We have examined the description of **Foresight Works Israel Ltd.** (hereinafter "*Foresight*") System Services based on the criteria set forth in paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the Security and Availability principles set forth in TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria), throughout the period January 1, 2025, to December 31, 2025.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of *Foresight* controls are suitably designed and operating effectively, along with the related controls of the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The controls included in the description are those that management of *Foresight* believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of the Data Center Services system that are not likely to be relevant to meeting the applicable trust services criteria.

Service Organization's Responsibilities

Within Section 2 of this report, *Foresight* has provided an assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. *Foresight* is responsible for

(1) preparing the description and assertion; (2) including the completeness, accuracy, and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria; and (6) specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA), and, accordingly, included

procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2025, to December 31, 2025.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves:

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2025, to December 31, 2025;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively;
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met; and
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in *Foresight's* assertion and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period January 1, 2025, to December 31, 2025;
b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 2025 – December 2025, and user entities applied the complementary user entity controls assumed in the design of Foresight's controls throughout the period January 1, 2025, to December 31, 2025; and

c. The controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 1, 2025, to December 31, 2025 if the user entities applied the complementary user entity controls assumed in the design of Foresight controls, and those controls operated effectively throughout the period January 1, 2025, to December 31, 2025.

Description of Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are presented in Section 4 of this report.

Restricted Use

This report is not intended to be and should not be used by anyone other than these specified parties.

RSM Shiff Hazenfratz & co., CPA

Tel-Aviv, Israel

June 13th, 2026

SECTION 3: FORESIGHT'S DESCRIPTION OF ITS INFRASTRUCTURE SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1,2025, TO DECEMBER 31,2025

General Background

Foresight Works Ltd ("Foresight" or "the Company") is a privately held company headquartered in London, United Kingdom, with operating entities in the United States and Israel.

The Company delivers AI-powered analytics and decision-support solutions to enterprise clients across multiple industries. Foresight operates a centralized infrastructure services system that supports the delivery of its software platform and professional services to customers globally.

The Company's executive leadership oversees the design, implementation, and operation of controls over the system throughout the reporting period.

Types of Services

The main types of services the company offers include:

(1) **SOFTWARE-AS-A-SERVICE (SAAS) PLATFORM ACCESS** – Foresight provides authenticated, role-based access to its hosted analytics and decision-support platform via secure web interfaces and APIs.

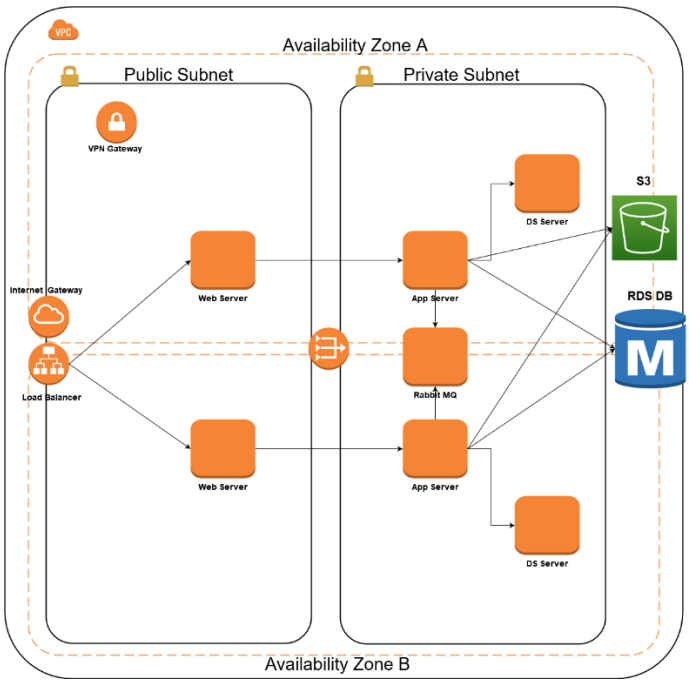
(2) **DATA INGESTION AND PROCESSING SERVICES** – Foresight processes customer-provided data through its platform to generate insights, reports, and analytical outputs.

(3) **CUSTOMER SUPPORT AND OPERATIONAL SERVICES** – Foresight provides technical support, account management, and onboarding services to clients via email, ticketing systems, and scheduled communications.

(4) **PROFESSIONAL SERVICES** – Foresight delivers configuration, integration, and advisory services on a Time and Materials or fixed-fee basis under separate engagement terms.

Infrastructure and Software

Below is the company's infrastructure chart:

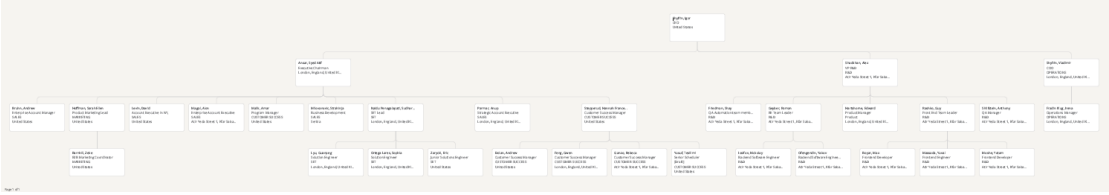


Among the main systems that are used by Foresight are as follows:

- **Cloud hosting and compute**: AWS EC2 for application workloads; AWS S3 for object storage; AWS for managed databases.
- **Networking and edge**: Load balancers, web application firewalls (WAF), and content delivery network (CDN) services to manage traffic and protect against common web threats.
- **Identity and access management**: Single sign-on (SSO) via Azure Active Directory, with multi-factor authentication (MFA) enforced for all production access.
- **Source control and CI/CD:** GitHub for version control, with automated build and deployment pipelines via Jenkins.
- **Monitoring and logging:** Zabbix for infrastructure and application monitoring; centralized log aggregation for security and operational events.
- **Endpoint and device management:** SentinelOne for managed endpoints; antivirus and EDR tooling deployed across the corporate fleet.
- **Productivity and collaboration:** Outlook 365 for email and document collaboration; Slack for internal communications; OneDrive for documentation.

People

Foresight staff currently constitute a relatively medium-sized company, and in constant growth. At present, the following chart presents the staff hierarchy:



Policies and Procedures

Formal IT policies and procedures exist that describe computer operations, change control, and data communication standards. All teams are expected to adhere to Foresight's policies and procedures that define how services should be delivered. Foresight has, among others, the following policies and procedures which are updated for 2025:

- Data Security Procedure
- Human Resources Security Policy
- Internal Audits Procedure
- Risk Assessment Policy
- Monitoring Policy
- Threat intelligence Policy
- Privacy Practices Policy
- Business Continuity Plan
- Secure Development Policy
- Incident Management Policy

Security

Foresight applies logical security controls in every aspect of the business processes. A designated HR system manages all access management for new employees and leaving employees. A quarterly access permissions review is performed to ensure that no unauthorized personnel have access to the organization network.

As for physical security, Foresight office is located at 7 Golda Meir St., Ness Ziona, Israel, for which all defined sensitive areas within the organization's facility are recorded by CCTVs. Entering the facility is only for authorized persons via PIN code that is known only by authorized persons, access management tracking, visitors badge accompanied with authorized personnel etc.

Risk Management

Foresight has designed and approved comprehensive information security procedures that cover all aspects of information security management within the organization, along with a Business Continuity Plan, Risk Management and Security Incident Management policies.

According to the procedure, the company conducts periodic risk assessments and risk management to scope all the potential threats that could affect the company. The last

Penetration Test for the platform was conducted during June 2025. As for risk assessment, it was conducted early Y2026 for which all risks were mapped, controls were tested, and the platform vulnerabilities were checked.

Complementary User Entity Controls

Foresight implementation of information technology and general IT controls are designed with the assumption that user entities will implement specific controls. Such controls are called complementary user entity controls. It is not feasible for all the control objectives related to Foresight general controls to be solely achieved by Foresight control activities. Accordingly, in conjunction with the information technology general controls system, user entities should establish internal controls or procedures to complement Foresight's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

- User entities are responsible for having procedures in place to properly segregate duties and help ensure only authorized personnel can perform sensitive functions and that access to these functions are periodically reviewed.
- User entities are responsible for enforcing the use of unique IDs and for configuring password parameters to any relevant system, or their directory service where a directory service sync is utilized, which authenticates users in accordance with their internal policies.
- User entities are responsible for choosing the type of permission given to their users.
- User entities are responsible for monitoring log-in attempts and enforcing workstations to automatically lock after a predetermined period of inactivity.
- User entities are responsible for the security of content once it is exported from Foresight platform.
- User entities (on prime system) are responsible for exporting Customer Data (forms and reports) for backup use or to backup Foresight Platform through the Customer server.
- Customers are responsible for implementing controls to ensure access for terminated users is removed timely.
- User entities are responsible for establishing adequate physical security and environmental controls of all devices and access points residing at their operational facilities.

SECTION 4: RELATED CONTROLS, TESTS OF CONTROLS AND RESULTS OF TESTS

Privacy & Confidentiality

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Communication	PC-1	The entity updates its customers regarding its privacy policy.	The organization's customers will be notified by email if there is a change in the privacy policy, and an update will also be made on the company's website.	Effective
	PC-2	The entity provides information to the relevant parties regarding the collection, use, storage and disposal of private information.	The organization signs an SLA as part of an agreement with its customers. In addition, there is a reference in the privacy policy regarding the organization's commitment to data deletion.	Effective
	PC-3	The entity may provide information to third parties only for the purposes specified in the notice and only with the express consent of the person.	Within the framework of contracts with suppliers, it is specified that the organization's suppliers cannot transfer the information to a third party without permission from the organization.	Effective
Information Security	PC-4	The entity secures and protects data against any unauthorized access.	The company implements strict security controls and protective measures, such as firewalls, antivirus solutions, and monitoring systems, to prevent unauthorized access to data (refer to the Information Security section).	Effective
	PC-5	Encryption is being held for confidential information coming out of the company	The company implements designed tools for encrypting data using HTTPS and TLS for data at rest and data at transit.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
	PC-6	There is encryption for sensitive information present on mobile devices and endpoints	The company implements designed tools for encrypting data using HTTPS and TLS for data at rest and data at transit.	Effective
Policies and Procedures	PC-7	The entity has a detailed privacy policy.	The organization has a detailed Privacy Policy that is published on the official site. In addition, the company conducts an annual review of the privacy policy and, if necessary, will make updates in accordance with changes in the law. https://www.foresight.works/privacy	Effective
	PC-8	Procedures in place for identifying and assigning confidential information once received or created and determining the period for which it should be kept.	The procedures are reviewed annually, and their classification level will be determined in accordance with the information classification procedure.	Effective
Supervision	PC-9	The entity collects and stores information only in accordance with the reasons appearing in the notice for the person and in whose name the information was collected.	Within the framework of the privacy policy, the organization details what information is collected and details the process for deleting the information.	Effective
	PC-10	The entity specifies the purposes for the collection, retention and disposal of data.	As part of the Privacy Policy, it is stated how long the organization will retain the data and how the deletion process will be carried out. The organization will retain the HR and financial information for 7 years in accordance with the law and then delete it.	Effective
	PC-11	The entity oversees and enforces its privacy policies and procedures.	The privacy policy is reviewed once a year and, if necessary, is updated and approved by a lawyer. If necessary, clients will be informed of the change.	Effective

Information Security

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Admins Monitoring	IS-1	There is an ongoing monitoring process for administrator users' actions in the organization	The company holds logs for all activities within all the systems in the organization via FW, including alarms for any abnormal activity.	Effective
Authorized Signatories	IS-2	There is a procedure for authorized signatories in the company that specifies the signature rights in the company, including the signing rights in the relevant information systems (such as an ERP system)	The company has a designed Signature Rights Document that lists all authorized signatories: * Igor - for England * Alex - for Israel	Effective
Backups and Restores	IS-3	The company has procedures regarding all aspects of backups, including the type of backup, schedules, saving backup tapes, etc.	The company has formal procedures in place governing all aspects of data backups, ensuring the availability, integrity, and security of the data.	Effective
	IS-4	There is a daily / weekly / monthly overview of the backups performed by the company to check the integrity and accuracy of the backups. Faults in the backup process are handled on an ongoing basis.	All backups are maintained according to relevant laws and regulation via AWS backup. The rest of the data is backed up according to the company's Information Security Procedures and Policies.	Effective
	IS-5	The company performs an initiation restoration periodically in order to check the backups.	The company operates in accordance with the backup procedure with regards to performing initiative restoration at least once a year, based on the risk rating.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
	IS-6	The company has a backup process for all information assets in the organization, with the backup being on a daily/weekly/monthly basis. The backup tapes are stored in a secure location in a remote site / in the cloud.	All backups are maintained according to relevant laws and regulation via AWS backup. The rest of the data is backed up according to the company's Information Security Procedures and Policies.	Effective
Cyber Incidents	IS-7	There is a procedure for handling an information security incident in the company	The company has a formal procedure for handling information security incidents that instructs employee on handling security events. All information security events are being documented in accordance with the procedure.	Effective
	IS-8	Security tools are deployed and system components are configured to monitor security-related events.	The company has a formal document that lists all the tools employed for maintaining information security (Firewall and Sentinel One).	Effective
	IS-9	Information security incidents are reported to management and the board of directors in accordance with company policies and procedures	There's a formal procedure for managing cyber incidents, including communication between employees and management. However, no incidents were reported in the last year.	Effective
	IS-10	There is an orderly communication process between the company's employees in the event of potential security breaches	There's a formal procedure for managing cyber incidents, including communication between employees and management. However, no incidents were reported in the last year.	Effective
	IS-11	There is an information security incident log review process to examine the types of incidents and raise the level of security accordingly	The control is implemented as described. However, no incidents were reported in the last year.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Information Security Officer	IS-12	The company has the role of Chief Information Security Officer (CISO) who is in charge of securing the organization's activities, managing cyber risks, preventing information leakage and embezzlement, managing security resources and access permissions in systems.	Boris Kogan is the CISO (outsourced) and the information security officer in the organization and has signed a letter of appointment as an information security officer. The letter of appointment was signed by the organization's VP R&D in Y2022.	Effective
	IS-13	The company's CISO establishes periodic meetings to discuss information security issues in the company	A semi-annual meeting is set up by the CISO to discuss information security issues in the company.	Effective
Physical Security	IS-14	The company has physical security measures such as cameras, fire extinguishers, guards etc.	The organization has all the required physical security measures such as cameras, guards, fire extinguishers, alarm system, access control via PIN code etc.	Effective
Policies and Procedures	IS-15	There are information security procedures in the company that include all aspects of information security management in the organization	The organization has information security procedures that are shared with relevant employees who are required to observe them. Also, the organization has an information security policy. Employees sign the Appendix Information Security Policy.	Effective
Risk Assessment	IS-16	A risk assessment is being conducted periodically to check the level of information security and risk management in the organization.	The company conducts a risk evaluation internally to check the level of information security and arrange controls according to a designed policy for Risk Management.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
	IS-17	An enterprise-wide risk assessment is performed annually by management, which includes setting business objectives and assessing the impact of environmental, regulatory and technological changes on the security of a company's systems.	The company conducts external risk assessments to identify potential risks the organization may face and implements controls accordingly. These assessments are updated annually. The last risk assessment was conducted during March 2025 where no material findings were detected.	Effective

Organization & Management

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Employees Evaluation	OM-1	There is a periodic employee evaluation process by their direct managers in order to set goals and examine the achievement of previous goals.	The organization maintains a structured annual employee evaluation process conducted by direct managers. This process occurs once a year when all direct managers set up goals for each employee on his staff.	Effective
Incorporation Document	OM-2	There is a document of incorporation for the company in which the role of the board of directors is defined.	The organization maintains an official incorporation document that clearly defines the role, responsibilities, and governance structure of the board of directors.	Effective
Organizational Hierarchy	OM-3	Roles and responsibilities in the organization are defined and documented.	Roles and responsibilities within the organization are clearly defined, documented, and regularly reviewed to ensure alignment with operational needs and security requirements.	Effective
	OM-4	The company has an organizational chart detailing the organizational hierarchy, the key areas and the communication between the company's employees.	The organization maintains an updated organizational chart detailing clear reporting structures, departmental hierarchy, and key personnel's roles and responsibilities.	Effective
	OM-5	The organizational chart is available to all company employees.	The organizational chart is maintained by the organization, regularly updated, and is readily accessible to all company employees via HR app.	Effective
Overlap	OM-6	When an employee leaves, there is an orderly process of overlapping between the departing employee and the new employee filling the position.	The organization maintains a well-organized and structured handover process between the direct manager of departing employees and their replacements.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Periodic Meetings	OM-7	Management updates employees at periodic meetings about new customers, new features, challenges, procedures, etc.	Management conducts weekly or bi-weekly meetings to ensure employees remain informed regarding updates about new customers, product features, current challenges, and policy or procedural changes.	Effective
Recruitment Process	OM-8	Background checks (recommendations, criminal record, polygraph, etc.) are performed for job applicants in the organization as a component in the recruitment process.	As part of the recruiting process, the company performs background checks that include credibility, previous workplaces recommendations, criminal check as part of clients' requirements, and social media check.	Effective
	OM-9	New employees are required to read and accept the physical security policy, the information security policy and the confidentiality agreement as part of the recruitment process.	As part of the recruitment and onboarding process, new employees are required to review and formally acknowledge the organization's IT policies and Confidentiality Agreement.	Effective
	OM-10	There is an orderly recruiting process in the company according to the requirements of each position so that at least 2 interviews are conducted with a technical test if necessary.	The organization maintains a structured and orderly recruitment process aligned with the specific requirements of each position. At least two interviews are conducted for each candidate.	Effective
Training	OM-11	Staff members are required to attend annual training on security, confidentiality and privacy issues.	All newly recruited employees must sign a complete information security training covering security, confidentiality, and privacy topics. Also, on an annual basis, all employees must complete an information security and privacy training. Training attendances are documented and tracked.	Effective

Risk Management

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
BCP	RM-1	The company has procedures and policies regarding business continuity and disaster recovery that list potential cases of disasters and how to deal with them.	The organization maintains comprehensive and documented Business Continuity and Disaster Recovery policies and procedures. These documents clearly identify potential disaster scenarios, outline specific response and recovery actions. The procedure was last updated during Feb-24. The procedure was also updated during Feb-26.	Effective
	RM-2	The company conducts training for its employees in all matters of business continuity.	The company conducts annual Business Continuity Procedure training for its employees to ensure they are familiar with the procedures and prepared to respond effectively in the event of an actual emergency.	Effective
	RM-3	The company conducts periodic exercises regarding the business continuity plan and updates the plan in accordance with the findings and recommendations.	The company operates in accordance with the Business Continuity Plan (BCP) procedure and conducts an annual live exercise by performing proactive restoration tests for all databases. All findings are documented and communicated to management along with relevant recommendations. The last BCP exercise was done during February 2025 where it was done without any material findings.	Effective
	RM-4	Findings and recommendations regarding business continuity practices and training are regularly reported to the Board of Directors.	The BCP exercises findings are presented to the management members for discussion.	Effective
	RM-5	Management reviews the Disaster Recovery and Business Continuity Plan on an annual basis to ensure it meets business requirements for customer availability.	The BCP procedure is updated on an annual basis and following the exercises recommendations if required.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Customer Contact	RM-6	There is a terms of use document that the customer needs to confirm when communicating or logging into the platform	The company has terms-of-use that are published on its official site. The terms are required to be confirmed by clients on the onboarding process as part of the agreement. https://www.foresight.works/terms	Effective
	RM-7	The terms-of-use document adequately defines the boundaries of the system and the customer's responsibilities, reference to information confidentiality and privacy.	The company has terms-of-use that is published on its official site. https://www.foresight.works/terms	Effective
External Suppliers	RM-8	External suppliers of the company perform a periodic risk assessment to check the level of security and continue to provide service to its customers	The company has mapped all critical suppliers in which all of them are required to complete an information security questionnaire to identify risks in their organizations. The main vendor of the company is AWS for which is considered a world-wide secured one. Another main system the company uses is Tactivision - system services, for which its security is checked.	Effective
	RM-9	Suppliers of the company are required to sign NDA / confidentiality / code of ethics documents	All suppliers identified by the company as critical are required to sign an NDA and complete an information security questionnaire, with the exception of Amazon Web Services, which is considered a trusted vendor.	Effective
Cyber Insurance	RM-10	The company has a Cyber insurance to cover specific damages caused by Cyber incident.	The company has valid cyber insurance to cover specific damages to which it might be exposed.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Monitoring	RM-11	The company has environmental monitoring systems that examine cases of: - Water leak - Air handling units - UPS systems - Generators	Irrelevant as the platform is cloud-based. Nevertheless, the sites are monitored for that matter.	Effective
Risk Assessment	RM-12	Risk assessment is performed annually and includes the identification and assessment of the risks associated with identified threats that may compromise the information security of the system. Management identifies controls that reduce the risks identified.	"The company conducts external risk assessments to identify potential risks the organization may face and implements controls accordingly. These assessments are updated annually. The most recent Penetration Test (PT) was conducted in June 2025, and there was a retest during August 2025. As for risk assessment, last one was conducted during March 2025 where no material findings were detected."	Effective
	RM-13	There are detailed and documented procedures regarding risk assessment and how to handle them for the purpose of guiding the company's employees in connection with monitoring, documenting and solving information security problems.	The organization maintains detailed and documented procedures for conducting risk assessments and managing identified risks.	Effective
	RM-14	The results of the risk assessment carried out by the Company are reported to senior management and the Board of Directors for discussion and implementation of recommendations.	On an annual basis, management conducts a review meeting to present and discuss the high-risk findings identified in the most recent risk assessment and penetration test (PT).	Effective

Physical and logical access control

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Access Control	LP-1	Access to the entity's ERP system is restricted through unique username and password entries.	Access to the company's platform is only authorized persons have access. The platform access is via username and password that defined by the AD password policy (SSO)	Effective
Access Control	LP-2	Requests to change access permissions are made by management, or by an authorized customer manager.	The company has a designed access management policy for granting and removing permissions. Any changes in access permissions must go by the procedure.	Effective
Access Control	LP-3	Access control system management is limited to IT, management and operations personnel.	Alex and Irena are the authorized personnels for managing access.	Effective
Logical Security	LP-4	The company has FW software that protects the company's network from intrusions. The system alerts and sends emails to defined people accordingly.	Firewalls are implemented to protect both the corporate office network through Sentinel One solutions and the cloud environment through Amazon Web Services Web Application Firewall (AWS WAF), in order to monitor, filter, and prevent unauthorized or malicious network traffic.	Effective
Logical Security	LP-5	Antivirus software is configured to monitor traffic within the internal network as well as communication with external networks, and to detect and prevent the transmission of data or files containing certain virus signatures identified by the antivirus software.	The company uses Sentinel One as its antivirus solution to protect and monitor the internal network against potential threats.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Logical Security	LP-6	Logical access to technical workstations is restricted by the following password requirements: - Minimum length of 8 characters - Expired after 60 days - A combination of alpha-numeric characters, upper and lower	Logging into workstations via MFA that includes among others a password created by designed policy.	Effective
	LP-7	Network policy is set to lock workstations after 15 minutes of inactivity.	Network policy is set to lock workstations after 15 minutes of inactivity.	Effective
	LP-8	Antivirus software is automatically updated with current virus signatures. A central server is utilized to push updates to production servers daily.	The AV is updated automatically on an ongoing basis.	Effective
Physical Security	LP-9	Each facility has an access control system to prevent the intrusion of unauthorized users and to restrict authorized users to appropriate areas.	Access to the company's facilities is restricted to authorized personnel only and is controlled via employee-specific ID cards unique to each individual.	Effective
	LP-10	The servers' rooms do not contain external windows.	Irrelevant as the company doesn't have a server room.	Effective
	LP-11	The company has physical security measures for entering the organization's environment. Access to the site is for authorized persons only.	There're security CCTVs, access management and tracking, entering via PIN code, alarm system, a guard etc.	Effective
Policies and Procedures	LP-12	Documented policies and procedures of physical security are intended to guide the activities of employees to provide, control, monitor and cancel physical access.	The company maintains documented physical security policies and procedures that guide employee behavior and establish controls for granting, managing, monitoring, and revoking physical access to company facilities.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Remote Access	LP-13	VPN sessions require unique usernames and password authentication.	VPN connection requires a username and a password, and only authorized personnels are able to remotely connect.	Effective
	LP-14	Remote access to technical workstations that enable an entity to provide remote support to customer systems is limited by secure VPN connectivity.	VPN connection requires a username and a password, and only authorized personnels are able to remotely connect.	Effective
	LP-15	Remote provider access to the company's network for limited support by secure VPN connectivity.	VPN connection requires a username and a password, and only authorized personnels are able to remotely connect.	Effective
Users Management	LP-16	There is an orderly process for opening a new username in the company's systems and granting permissions according to the role of the new employee.	Through the designated HR system, each employee receives a username, password, and access permissions aligned with their job role upon recruitment.	Effective
	LP-17	There is an orderly process for closing a user in the company systems for an employee who has left.	Through the designated HR system, employee access permissions are removed or revoked in accordance with the employee’s termination date and role requirements.	Effective
	LP-18	Every year, the list of users in the company's systems is reviewed to check user privileges.	Once on quarterly basis, the IT staff performs an access permissions review on all systems. However, the last access permission was conducted during March 2026.	Effective
Visit Procedures	LP-19	Visitors, suppliers and contractors are required to: - View ID - Sign up for visit approval, including name, company represented, site staff confirming access - Wear a visitor's badge to gain access into the facilities	All visitors have to be accompanied by authorized personnel and provide an ID for a deposit.	Effective

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
	LP-20	Visitors are required to be with a badge and accompanied by an authorized employee when accessing the facilities. And upon departure of the visitor, he is required to return the badge.	All visitors have to be accompanied by authorized personnel and provide an ID for a deposit.	Effective
	LP-21	Customer equipment resides in locked and separated environments within the data centers.	Each customer is separated into their environment (different network in a domain).	Effective
Workstations Security	LP-22	Workstations are restricted to authorized employees using unique usernames and passwords.	The company enforces strict access controls on all organizational terminals. Each employee is assigned a unique user account protected by a strong password policy.	Effective

Systemic Activity

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Control Management	SA-1	There is a system in the company that is used to monitor the following performance, availability and audited events for the services infrastructure: - Network availability - Hosting services and ports - CPU and hard disk utilization	The company monitors all infrastructure via Tactivision that summarizes the status of the cloud infrastructure.	Effective
Jobs Management	SA-2	The entity has procedures for scheduling automated tasks (scheduling jobs) and manuals.	No automated jobs other than authorized backup processes are permitted to run within the platform.	Effective
	SA-3	Jobs updates are performed by authorized persons only.	Only Alex is the authorized personnel to configure automated jobs.	Effective
	SA-4	There is a job management system that alerts you when there is a malfunction in a job run.	In case of a malfunction, the platform sends an alert to the IT staff for treatment.	Effective
Technical Support	SA-5	The technical support team is available 24/7 to manage data center monitoring systems that include electricity, temperature, humidity, video surveillance and access control.	Technical support is provided during working hours. However, the company respond immediately to any urgent call. As for monitoring physical measures, the facility has the relevant measures (except for temperature and humidity for which there are no physical servers).	Effective

Change Management

Sub-Topic	Test ID	Expected Control	Actual Control/ Entity Respond	Effective\ Ineffective
Changes Management	CM-1	Every change in the system goes through a designed process: request, approval, development, testing and approval of airing. The change management process is documented and maintained.	All developments are documented via JIRA. The development process includes: * Change request and approval * Development process * QA tests * Approval for Production Deployment by the CPO	Effective
	CM-2	There is a periodic review of the log of systems changes made during that period. The review is approved by authorized sources.	A log monitoring audit is performed by the IT manager once a year. However, the last changes log review was conducted during Mar-26.	Effective
Communication	CM-3	The organization updates customers on changes / updates made to the system.	The product manager sends out an email regarding new versions for all clients.	Effective
Environment Separation	CM-4	There is a separation of environments in the company's systems; Production, development and testing.	There are 3 separate environments: production, test (staging) and development (sandbox).	Effective
Policies and Procedures	CM-5	There is a procedure for managing changes in the company's systems that is updated once a period.	The company maintains a formal Change Management Procedure that governs the process of proposing, reviewing, approving, testing, and implementing changes to systems, infrastructure, and applications in a controlled and consistent manner.	Effective
Segregation of Duties	CM-6	There are no access permissions for IT personnels to the production environment.	The IT staff (12 employees) don't have full access to the production environment. Their access is merely for confirming a development to implement on production environment.	Effective