SOC 2 Type II Report

For the period December 1, 2025 to February 28, 2026

Report on Controls Placed in Operation at Limy AI Inc. and Limy Analytics Ltd. Relevant to Security, Availability and Confidentiality with the Independent Service Auditor's Report Including Testing Performed and Results Thereof

Table of Contents

Limy

Section I – Limy AI Inc. and Limy Analytics Ltd.’s Management Assertion

March 30, 2026

We have prepared the accompanying description titled "Description of the Limy AI Platform relevant to Security, Availability and Confidentiality throughout the period December 01, 2025 to February 28, 2026" (Description) of Limy AI Inc. and Limy Analytics Ltd. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Limy AI Platform (System) that may be useful when assessing the risks arising from interactions with the System , particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Carved-out Unaffiliated Subservice Organization: Limy AI Inc. and Limy Analytics Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The Description indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Limy AI Inc. and Limy Analytics Ltd. to achieve Limy AI Inc. and Limy Analytics Ltd.’s service commitments and system requirements, based on the applicable trust services criteria. The Description presents Limy AI Inc. and Limy Analytics Ltd.’s controls and the types of complementary subservice organization controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.’s controls. The Description does not disclose the actual controls at the carved-out AWS.

Complementary user entity controls: The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Limy AI Inc. and Limy Analytics Ltd.’s controls to achieve the service commitments and system requirements. The Description presents Limy AI Inc. and Limy Analytics Ltd.’s controls and the complementary user entity controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.’s controls.

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

a. The Description presents the System that was designed and implemented throughout the period December 01, 2025 to February 28, 2026 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period December 01, 2025 to February 28, 2026 to provide reasonable assurance that Limy AI Inc. and Limy Analytics Ltd.’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if user entities applied the complementary user entity controls and the carved-out subservice organization applied the complementary controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.’s controls throughout that period.

c. The Limy AI Inc. and Limy Analytics Ltd. controls stated in the Description operated effectively throughout the period December 01, 2025 to February 28, 2026 to provide reasonable assurance that Limy AI Inc. and Limy Analytics Ltd.’s service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary user entity controls and the complementary carved-out subservice organization controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.’s controls operated effectively throughout that period.

Ori Riechman, CTO

Shape the future with confidence

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Section II – Independent Service Auditor

To the Management of Limy AI Inc. and Limy Analytics Ltd.

Scope

We have examined Limy AI Inc. and Limy Analytics Ltd.'s accompanying description titled "Description of the Limy AI Platform relevant to Security, Availability and Confidentiality throughout the period December 01, 2025 to February 28, 2026" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*, (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period December 01, 2025 to February 28, 2026 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA Trust Services Criteria.

Carved-out Unaffiliated Subservice Organization: Limy AI Inc. and Limy Analytics Ltd. use AWS (subservice organization) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Limy AI Inc. and Limy Analytics Ltd., to provide reasonable assurance that Limy AI Inc. and Limy Analytics Ltd.'s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents Limy AI Inc. and Limy Analytics Ltd.'s system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed and are operating effectively at AWS. The Description does not disclose the actual controls at AWS. Our examination did not include the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period December 01, 2025 to February 28, 2026.

Complementary user entity controls: The Description indicates that Limy AI Inc. and Limy Analytics Ltd.'s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Limy AI Inc. and Limy Analytics Ltd.'s responsibilities

Limy AI Inc. and Limy Analytics Ltd. 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 its service commitments and system requirements were achieved. Limy AI Inc. and Limy Analytics Ltd. has provided the accompanying assertion titled, Limy AI Inc. and Limy Analytics Ltd.'s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Limy AI Inc. and Limy Analytics Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated therein to achieve the service organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") . Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period December 01, 2025 to February 28, 2026. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Our examination was not conducted for the purpose of evaluating the performance or integrity of Limy AI Inc. and Limy Analytics Ltd.'s AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Limy AI Inc. and Limy Analytics Ltd.'s AI services.

We are required to be independent of Limy AI Inc. and Limy Analytics Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and

system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the service commitments and system requirements based on the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. the Description presents the Limy AI Platform system that was designed and implemented throughout the period December 01, 2025 to February 28, 2026 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed throughout the period December 01, 2025 to February 28, 2026, to provide reasonable assurance that Limy AI Inc. and Limy Analytics Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.'s controls throughout that period.

c. the controls stated in the Description operated effectively throughout the period December 01, 2025 to February 28, 2026 to provide reasonable assurance that Limy AI Inc. and Limy Analytics Ltd. service commitments and system requirements were achieved based on the applicable trust services criteria if the complementary subservice organization and user entity controls assumed in the design of Limy AI Inc. and Limy Analytics Ltd.'s controls operated effectively throughout that period.

Restricted use

This report , including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Limy AI Inc. and Limy Analytics Ltd., user entities of Limy AI Inc. and Limy Analytics Ltd.'s Limy AI Platform system during some or all of the period December 01, 2025 to February 28, 2026 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization
- how the service organization's system interacts with user entities, subservice organizations, or other parties
- internal control and its limitations
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- user entity responsibilities and how they interact with related controls at the service organization
- the applicable trust services criteria
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global Limited

Shape the future with confidence

March 30, 2026
Tel-Aviv, Israel

Section III – Description of the Limy AI Platform relevant to Security, Availability and Confidentiality throughout the period December 01, 2025 to February 28, 2026

Purpose and Scope of the Report

This report covers the services provided to customers by the Limy Service hosted on Amazon Web Services (AWS).

Note: Parenthetical references in this report are cross-references to the applicable control procedures included in the Description of Criteria and Controls section at the end of this report.

Company Overview and Background

Founded in 2025, Limy is privately held with locations in New York City (169 Madison Ave) and Tel Aviv (9 Tversky St). The company is backed by a16z, Flybridge, AnD Ventures and Axium.

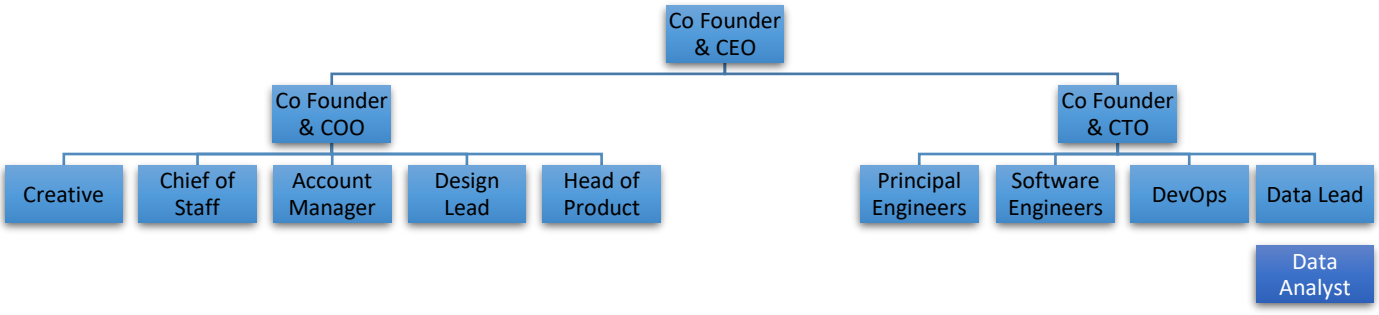
Products and Services

Limy is building a platform that helps companies stay in control in the agentic web era - where AI agents decide what gets surfaced. With a unique data infrastructure and proprietary technology, Limy enables brands to measure attribution across AI shopping flows, run product visibility campaigns, and control how their items, descriptions, and categories surface inside LLM-driven recommendations.

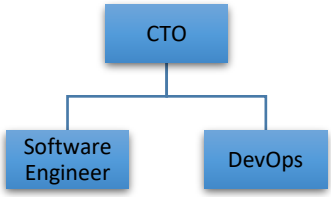
Organizational Structure

Limy's organizational structure provides the overall framework for planning, directing, and controlling operations by segregating duties between business functions. Segregation of duties processes are maintained to reduce the risks of unapproved and unauthorized changes. Limy's Operations department receives supporting services from other Limy departments, such as Research and Development (R&D), Sales, and Marketing. An organizational chart is maintained and clearly defines management authority and reporting structure (**9**).

Organization Structure: High Level



R&D Structure



Job Description and Responsibilities of the Operations Team:

CTO	● Provides leadership and develops objectives for the service department. ● Obtains funding for existing and future projects. ● Develops and directs the design and development of new products and improves existing products. ● Works with members of the senior management team to further departmental and company goals. ● Plans to support future growth and expansion. ● Takes ownership of projects to improve Limy's operations. ● Builds a skillful and responsible Dev team.
Software Engineer	● Responsibility for Limy's 24/7 multi-site cloud operations. ● Handles exceptions and operational requests in Limy's production environment. ● Implements and uses monitoring tools. ● Automates configuration management and deployment. ● Builds, scales, and optimizes critical production systems. ● Builds out and maintains disaster recovery (DR) for Limy's production environments. ● Ensures the security of Limy's critical systems. ● Maintains continuously involved with the larger Dev community and contributes the best practices to Limy.
DevOps	● Takes part in the product design and planning phases. ● Develops complex systems and services that are deployed in production at scale. ● Fixes and improves existing software where required. ● Researches new technologies. ● Analyzes and studies complex systems requirements.

Description of the Production Environment

Production Environment

Limy executes the processes described below by using a secure-cloud service platform. The platform complies with standards of quality, security, and reliability that enable Limy to provide its services efficiently and dependably. Limy protects confidential information against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition, according to confidentiality commitments and requirements.

Note: Controls performed by the data center service providers are not included in the scope of this report.

Network Infrastructure

A robust network infrastructure is essential for reliable and secure real-time data communication between Limy's cloud service components. To provide sufficient capacity, Limy's network infrastructure relies on a secure-cloud service platform. To ensure a secure network, Limy's standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, and ensuring confidentiality, integrity, and availability.

Limy's security components:

- Application layer security:
  - Various authentication schemas (multi-factor authentication (MFA), unique ID and a complex password policy)
  - Logical security
  - Penetration testing

- IP address source restriction
- Customer data encryption at-rest and in transit

- Network and infrastructure security:
  - Network architecture
  - Risk management
  - AWS data centers
  - Cloud operation security (change management, monitoring and log analysis)

Web, Application and Service Supporting Infrastructure Environment

Limy utilizes clustered infrastructure design to provide redundancy and high availability. In addition, the infrastructure enables auto-scaling capabilities. This allows high performance during demand spikes to the services.

Overview of Company's Internal Control

The Board of Directors, management and other personnel manage the process of internal control, which is designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. These are the six components of internal control at Limy:

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for the components of internal control, providing discipline and structure. The protection of assets from unauthorized use or disposition is executed in accordance with management's authorization and customer instructions. Limy's management maintains an internal control structure that monitors compliance with established policies and procedures. Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal (**4**). The internal control structure is refreshed annually based on Limy's assessment of risks facing the organization.

Management sets the tone on integrity, ethics, and competence of Limy's employees, policies and procedures, risk management process and monitoring, and the roles of significant control groups. Below are the categories that define management's tone:

Authority and Responsibility — Lines of authority and responsibility are clearly established throughout the organization and are communicated through Limy's: (a) management operating style, (b) organizational structure, (c) employee job descriptions, and (d) organizational policies and procedures.

Corporate Governance and Strategy – Limy's control environment is influenced by its Board of Directors. The Board of Directors of Limy consists of the co-founders (CEO, COO and CTO) alongside directors, bringing many years of accumulated industry experience and expertise in various business aspects – spanning artificial intelligence, enterprise technology, digital marketing, and venture capital. The Board is actively involved in, and continually scrutinizes, the activities of Limy's functional groups, and acts with respect to its fiduciary responsibilities. Additionally, the Board raises questions and pursues key initiatives with management, as well as interact periodically with the external auditors. The Board of Directors meets on at least an annual basis. The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions (**2**).

Management Philosophy and Operating Style – The Management Team, chaired by the CEO, has been delegated by the Board the responsibility to manage Limy and its business on a daily basis. The Management Team designs policies and communications so that personnel understand Limy's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Company management meets at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates (**3**).

Integrity and Ethical Values – Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Management may remove or reduce inappropriate incentives, extraneous pressures, or opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. In addition, management communicates Limy's integral values and behavioral standards to personnel through executive policy statements. The Board and management recognize their joint responsibility in fostering a strong ethical environment within Limy, to ensure that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Human Resource Policies and Practices – Human resource ("HR") policies include practices related to hiring, orienting, training, evaluating, counseling, promoting and compensating personnel. An essential element of the control environment is the competence and integrity of Limy's personnel. Job descriptions are documented and available on the company's website (**17**). All new employees undergo appropriate reference checks as part of the hiring process (**5**). In accordance with company policies, all new hires are required to sign a standard employment agreement that outlines confidentiality, Information Protection Awareness and the intellectual property clauses (**1**). Teams are expected to adhere to Limy's global policies that define how services should be delivered. These policies are documented on Limy's internal network and can be readily accessed by relevant Limy team members.

Commitment to Competence

Competence at Limy is designed to (a) identify and hire competent personnel, (b) provide employees with the training and information they need, (c) evaluate the performance of employees to determine their ability to perform job assignments, and (d) identify opportunities for growth and job performance improvement through the performance evaluation process. New employees complete a formal onboarding process documented through an onboarding checklist, which includes required steps such as the receipt of company-issued equipment (**6**). Professional training is provided based on development needs or operational demands. Training materials, guidelines, and relevant documentation are made available through the company's knowledge management portal (**7**). Employees are subject to a periodic feedback process (**10**).

Risk Assessment Process

The process of assessing risks is a critical component of Limy's internal control system. Risks and threats are evaluated by Limy's Risk Assessment team during a quarterly risk assessment meeting. The team reviews vulnerability reports and monitoring tools in relation to the organization's system security, availability, confidentiality, and privacy policies. In addition, the team monitors environmental, regulatory, and technological changes. Their effects are assessed, and their policies are updated accordingly. Once a year, the senior management reviews and approves the Yearly Risk Assessment report.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out. Control activities, whether automated or manual, generally relate to the achievement of specific control objectives and are applied at various organizational and functional levels.

Information and Communication

Management implements various methods of internal communication to enable employees to understand their roles and responsibilities and to communicate important issues in a timely manner. These methods include orientation and training programs for new employees, regular meetings, email messages, and more.

General Company Policies

Limy has established policies that govern the use of its information security systems. These policies are reviewed and approved yearly by the Management Team. The policies apply to employees, contractors, and temporary employees alike. Limy may update and amend these policies from time to time as circumstances and technologies develop.

It is the employee's responsibility to be aware of and comply with these policies. Failure to observe these policies may result in disciplinary action, up to and including termination, whether or not it causes any liability or loss to the company, and it may be performed at the company's discretion.

Communication

Internal communication

Management promotes effective communication within the organization. This involves producing and delivering messages and campaigns, facilitating intra-company dialogues, and establishing policies, processes and procedures. These policies, processes and procedures are communicated to employees through the company's internal portal. The Company maintains an architecture diagram that illustrates system components and security and protection measures for system resources (**11**).

External communication

External communication is defined as the transmission of information between the company and another entity in the company's external environment, such as customers, potential customers, suppliers, investors, shareholders, and society at large. The Company provides customer-facing "How-To" guidance through the website (**12**). Significant new features are communicated to customers through designated communication channels in accordance with the company's communication procedures (**13**). Furthermore, a dedicated communication channel is available to customers (**14**)**.**

Limy Operations - Criteria and Controls

The Trust Services Criteria and the controls that meet the criteria are listed in the Description of Criteria and Controls at the end of this document. The Limy Application and supporting control procedures are described using the following criteria:

- Limy's policies relevant to security, availability, confidentiality, and privacy
- Security procedures
- Software development lifecycle and infrastructure change management procedures
- Availability procedures
- Confidentiality procedures
- Monitoring procedures

Limy's management has specified controls to achieve these criteria. Note that certain Limy customers may have contracted with additional service organizations in conjunction with the services provided by Limy. The accompanying description includes only Limy's controls, not the related controls of any other service organizations that Limy or Limy's customers may have contracted out.

Limy's Policies Relevant to Security, Availability and Confidentiality

Formal written policies for the Trust principles and processes within the organization are developed and communicated so that personnel understand Limy's objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. Significant components of these policies include:

- Security, availability and confidentiality requirements of users
- Protection requirements, access rights, access restrictions, retention, and destruction
- Risk assessment
- Preventing unauthorized access
- Adding new users, modifying access levels, and removing users
- Assigning responsibility and accountability for system availability and confidentiality
- Assigning responsibility and accountability for system changes and maintenance
- Testing, evaluating, and authorizing system components before implementation
- Addressing how complaints and requests are resolved
- Identifying and mitigating Security, Availability and Confidentiality breaches and other incidents

- Training and other resources to support system security policies
- Handling of exceptions and situations not specifically addressed in policies
- Identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
- Sharing information with third parties
- Recovering and continuing service in accordance with customer commitments or other agreements
- Monitoring system capacity

Security and Architecture

Limy provides a secure, reliable, and resilient Software-as-a-Service (SaaS) platform that has been designed from the ground up based on industry best practices. Below are the network and hardware infrastructure, software, and information security elements that Limy delivers as part of this platform. Access to system resources is protected through a combination of enforcement points, remote connections, a native operating system security, database management system security, application controls, and intrusion detection monitoring software.

Data Center Infrastructure

Limy relies on Amazon Web Services (AWS) global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: FedRAMP, HIPAA, ISO 27001:2013, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS and more. AWS constantly updates its compliance programs.

AWS Data Centers

AWS data centers serve the highest industry standards in perimeter, infrastructure, data and environmental layers. The Company conducts annual evaluations of vendors and suppliers to confirm that their controls align with company policies and requirements (**16**), monitoring and logging of data center access, surveillance and detection, device management, operational support systems, infrastructure maintenance, and governance and risk. The Company conducts an annual review of the data center vendor's SOC2 report. Any identified deviations are reviewed and investigated as appropriate. The review includes identifying and documenting the controls implemented by the Company to address applicable Complementary User Entity Controls (CUECs) (**30**). AWS constantly updates its efforts and controls.

Data Centers – Physical Security

Access is scrutinized – AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who need to be present at a data center have to first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once the necessary work is completed.

Entry is controlled and monitored – Entering the Perimeter Layer is a controlled process. AWS staffs entry gates with security officers and employs supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas.

AWS data center workers control - AWS employees who routinely need access to a data center are given permission to enter relevant areas of the facility based on job function. But their access is regularly scrutinized. Staff lists are routinely reviewed by an area access manager to ensure each employee's authorization is still necessary. If an employee does not have an ongoing business need to be at a particular data center, they have to go through the visitor process.

Monitoring for unauthorized entry - AWS is continuously watching for unauthorized entry on its property, using video surveillance, intrusion detection, and access-log monitoring systems. Entrances are secured with devices that sound alarms if a door is forced or held open.

Environmental Protection

Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to an N+1 standard.

Fire Detection and Suppression – Automatic fire detection and suppression equipment has been installed to reduce risk.

Redundant Power – The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature Controls – The data center maintains a constant operating temperature and humidity level for all hardware.

Limy Offices

Physical access to company offices is restricted to authorized personnel through a designated access control system. Access is granted to company employees only, and all visitors are required to be escorted by a company employee at all times while on the premises (**29**).

Infrastructure Security

End-to-End Network Isolation – The Virtual Private Cloud is designed to be logically separated from other cloud customers in order to prevent data within the cloud from being intercepted. This isolation is achieved through the use of dedicated virtual networking components, including private subnets, routing controls, and access control mechanisms that restrict traffic flow both between environments and to the public internet. Internal services communicate only over private network paths, with no exposure to external networks unless explicitly required and secured. Ingress and egress traffic is tightly controlled to ensure that only authorized and necessary communication is permitted, further reducing the risk of unauthorized access or data leakage.

Network Security – Access to system resources is protected through a layered approach that includes enforcement points, secure remote connections, native operating system safeguards, database management system security measures, and application-level controls. Firewalls are configured to restrict unnecessary ports, protocols, and services (**28**). All servers are protected by tightly scoped network access rules, allowing only minimal required communication to and from the servers. The configuration of these access rules is tightly controlled and limited to authorized personnel.

Server Hardening – Servers are hardened according to industry best practices. This includes disabling or removing unused services and software, enforcing strong authentication and authorization mechanisms, applying the principle of least privilege, and ensuring timely patching of operating systems and installed components. Configuration baselines are reviewed regularly to maintain consistency, reduce the attack surface, and prevent misconfigurations that could lead to vulnerabilities.

Intrusion Detection – Intrusion detection systems are used to provide continuous monitoring of the company's network and to detect potential security breaches (**37**). Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks (**34**). Similarly, operational activities within the production environment are monitored and logged. Logs are reviewed by a designated team, and alerts are generated upon detection of anomalous activity (**32**).

Denial of Service (DoS) Protection – AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response is initiated. In addition to the DoS prevention tools, redundant telecommunication providers monitor each region as well as protect against the possibility of DoS attacks. In case of a DoS attack, an incident notification is sent to the designated group.

Segregation between Office and Production Networks – There is a complete separation between the corporate network and the production networks. Security practices enforce logical separation between different environments, such as Development, Testing, Staging, and Production (**20**). The access to the networked resources management platform is restricted to authorized personnel. Access to the production environment and database

is granted upon job requirements. Data transmitted between the company's customers and the application is encrypted using an authenticated TLS tunnel (**47**).

Penetration Tests – A penetration test is performed at least annually. Any identified high-severity findings are investigated and remediated through the SDLC process or other appropriate measures (**36**). The penetration tests are performed by an internationally acclaimed information security consultancy group. Any critical and high-risk security vulnerabilities are mitigated as soon as possible and after each penetration test.

Antivirus – An antivirus solution is installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software (**33**).

Application Security

Access Control – Access to Limy's services is through an identity-protected web application with full SSL security. Only authorized members of a specific organization have access to the organization's data. Organization administrators can disable access for users at any time. The application implements strict user access-control policy. For example, access to source code repositories requires MFA and is restricted to authorized users. Also, access to modify branch configuration within the source code management tool is restricted to authorized users to ensure proper segregation of duties (**25**). Access to build tools requires MFA and is restricted to authorized users as well (**26**).

Data Encryption – All traffic between the customer's client and the Limy platform is encrypted through TLS1.2 with only the most secure algorithms enabled. Encryption between Limy customers and the Application as well as between Limy's sites is enabled using an authenticated TLS tunnel. Customer data at rest is encrypted and hosted in secured storage services (**48**).

Vulnerabilities Management–Limy employs configuration management systems, including infrastructure-as-code tools, to enforce predefined configurations and maintain desired patch levels across all servers and software components. Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline (**35**). This approach ensures the timely identification, evaluation, and remediation of security vulnerabilities throughout Limy's IT systems, applications, and infrastructure.

Segregation of Customer Data – Limy employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated annually by third-party security consultants.

Operational Security

Identity and Access Management – Access to the AWS production environment requires Multi-Factor Authentication (MFA) and is restricted to authorized users (**23**).

Password Policy – Users are authenticated using unique user IDs and passwords via an Identity Provider (SSO) and/or directly within systems. Passwords are configured to meet defined security requirements (**22**).

Recertification of Access Permissions – Limy has implemented a recertification process to help ensure that only authorized personnel have access to the systems, environments, and databases. Permissions to production-related systems are reviewed, approved, and documented by Company management at least annually by the CTO (**27**). New employees are granted access to the different environments upon job requirements based on the employee permission table (**21**). The approved request - including the detailed permissions - is sent to CTO, who sets up the new user accordingly. Access to production-related systems is revoked upon employee termination. Company-issued equipment is returned in a timely manner, as documented in the offboarding checklists (**31**). Equipment that has handled sensitive information is disposed of only after ensuring that all such data has been securely erased. This includes revoking access permissions to systems and facilities and ensuring the return of all company property and equipment.

Security Incident Response Management – Whenever a security incident of a physical or electronic nature is suspected or confirmed, Limy's engineers are instructed to follow appropriate procedures detailed in the Security Incident Response Policy. Customers and legal authorities will be notified as recurred by privacy regulations.
Laptop Encryption – All company laptops are encrypted to protect sensitive information. Encryption is enabled and must remain active to ensure the confidentiality of customer and company data.

Data Encryption

Limy uses AWS APIs to manage services either directly from applications or third-party tools (e.g., software development kits [SDKs], AWS command line tools). TLS sessions are established between the client and the specific AWS service endpoint, depending on the APIs used, and all subsequent traffic, including the SOAP/REST envelope and user payload, is protected within the TLS session. Customer data at rest is encrypted and hosted in secured storage services.

Security and Privacy Awareness Training

The protection of sensitive data and maintenance of a high level of security awareness demands regular training of all employees to review handling procedures for sensitive information and hold periodic security awareness. All employees receive annual security awareness training and are required to acknowledge completion (**8**). Management reviews and updates the Security and Privacy Awareness Training protocol annually, or when relevant, to include newly developed security standards, and distribute them to all employees and contracts as applicable.

Software Development Lifecycle and Change Management (SDLC)

At Limy, software development and change management processes are designed to ensure that applications are properly planned, tested, approved, and aligned with the company's business objectives. The Company maintains a documented Change Management Policy, which is reviewed and approved at least annually (**39**). Multiple teams participate in the Software Development Life Cycle (SDLC) and change management activities. Both application and system infrastructure changes follow the same structured SDLC process. Responsibilities for the design, development, implementation, and ongoing operation of systems are clearly assigned and documented within the SDLC platform.
Furthermore, any changes that could impact system security, availability, confidentiality, or privacy are communicated to relevant management and affected users. Privacy impacts and potential risks are thoroughly assessed to ensure compliance with applicable privacy regulations.

Change Initiation

Changes are documented by opening a ticket within the SDLC Application. Decisions to approve, reject, or prioritize requirements are made by relevant personnel after assessing the change's potential impact (security, availability, confidentiality, and privacy). Once approved, related tasks are created in the SDLC App, and a developer is assigned to implement the change. The developer documents the scope, dependencies, and risks, and outlines the plan, including rollback procedures.
The developer works on the change within a dedicated branch and ensures that all updates are properly documented and tested before requesting a review. Each change is linked to its corresponding ticket for traceability. Automated tools support this process by performing preliminary quality and security checks before the code proceeds to the review phase.

"Pull Request" – Code Review

Changes to supporting infrastructure are documented in a centralized change management tracking system and are reviewed and approved prior to implementation. At least one reviewer examines the PR for correctness, security, and compliance with coding standards. All reviewer comments are documented, addressed, and resolved before approval. Once approved, the code is merged into the designated branch.
After merging, automated CI/CD pipelines execute acceptance and regression tests to verify stability. Alerts are sent to stakeholders on test failures. Design, implementation, configuration, modification, and management of infrastructure

and software are documented and approved through the change management application. Change management tickets are prioritized and labeled based on development phase and urgency. Infrastructure changes follow the same process as code changes.
Automated tests are performed using a designated tool to validate code quality. Code review is mandatory as part of the SDLC and is documented within the source control system. Successful completion of required tests is mandatory before continuing the SDLC process and deploying changes to the production environment. Change management tickets are linked to the source control system to associate each request with the corresponding code change. (**40**). Once merged and validated, the associated ticket in the SDLC App is updated to 'Done'. All PRs, reviews, and test results are retained for audit and traceability purposes.

Automatic Testing and Quality Validation

Throughout the SDLC process, automated tests are executed using dedicated tools to validate code quality and security. Tests occur during PR creation, post-merge, and pre-deployment. Alerts are issued for any failures to ensure timely remediation. Only code that passes all required automated and manual checks proceeds to production deployment.

Deployment to Production

Deployments to the production environment may be initiated only by authorized personnel or through an approved Continuous Deployment (CD) pipeline. Deployment is allowed only after successful completion of all required checks (builds, tests, security scans, and approvals). The CD system enforces these gates and records what is deployed, which commit, and when. Upon completion of deployment, a success notification will be sent to relevant stakeholders.

Infrastructure Change Management Overview

The company regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration of the existing components or performing routine maintenance activities, software updates, and other infrastructure-related changes according to available possibilities provided by the cloud platform provider. Infrastructure changes are documented within the Change Management tool. The request is reviewed and approved by the DevOps.

Emergency Changes

Emergency changes may be performed when it is the only way to solve a problem disrupting the Application's operation and services in a reasonable time. In this case, the development team will perform the necessary changes and then inform the relevant managers. After the change is completed, relevant personnel will determine a permanent course of action to solve the problem (e.g., whether to back out the emergency fix or allow it to remain in effect).

Availability Procedures

Limy hosts its production environment in the Amazon Web Services (AWS) located in N.Virginia, US. The production environment is fully managed by Limy's DevOps.

The production environment is comprised of numerous components, such as web services, application and data server types, databases, monitoring tools, and redundant network services. Limy maintains a dedicated DevOps Team to provide service availability to customers, and to support the operations of the Limy environment.

The company uses a set of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders through an internal communication tool, based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency. In addition, the DevOps Team is responsible for investigating escalated issues. Limy recognizes that backup and maintenance of data is critical to the operations of Limy's services. It is essential that industry best practices

be followed to ensure that data is backed up on a regular basis, and the integrity of the procedure is sound. The DevOps Team is also responsible for managing and backing up various types of service-related procedures.
Uptime commitments to customers are defined in the applicable SLA agreements (**43**). The Company monitors system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications are communicated to customers based on management's determination (**42**). Opening an incident ticket is done manually by one of Limy's employees in cases of (a) breaches of the system security, (b) availability, (c) confidentiality, and (d) customers reported issues.

Database Backup (DB)

Database servers at the data centers are located in secured locations with security measures implemented to protect against environmental risks or disasters. Limy utilizes relational, as well as NoSQL, databases that manage backups, software patching, automatic failure detection, and recovery. The DB instances are configured in a private-facing subnet with no internet access. To architect for high availability, Limy runs DB instances in several availability zones using Multi Availability Zones (AZ) deployment and utilizing the AWS automatic provisioning to maintain a synchronous standby replica of their DB instances in different availability zones.

The primary DB instance is synchronously replicated across availability zones to the standby replica, in order to provide data redundancy, failover support and keep the system fully operational during system backups. Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.
In case of a planned database maintenance, DB instance failure, or an infrastructure failure, Limy's database infrastructure allows failover (Disaster Recovery) to the standby site, so that they can resume database operations as soon as the failover is complete.

Limy's databases are configured to perform a daily snapshot of the data. DB instance backups are retained for a limited period (i.e., a retention period) and are verified periodically. The backup system automatically generates a backup log, which is reviewed by the DevOps team to verify that the backup has been successfully completed. Failures, if any, are identified by a success/fail notification and resolved in the next day's backup cycle.
Limy's Recovery Time Objective (RTO) is 12 hours, and its Recovery Point Objective (RPO) is 24 hours.

To protect data at rest, Limy deploys industry-leading encryption algorithms to secure customer data, files and media that reside in Limy storage systems. All data is encrypted with advanced encryption standards. Limy uses role-based access control to control access to database resources and API actions, especially actions that create, modify, or delete data resources, and actions that perform common administrative tasks, such as backing up and restoring DB instances. Following the least-privilege principle when granting permission using Identity and Access Management (IAM) policies, Limy controls the actions that users and groups can perform on the database resource. The Company performs backups of its application database to support data availability and recovery (**44**). The backups are stored on the AWS Cloud platform.

Restore

Limy validates the backup process by performing a backup restore procedure, known as – the Data Recovery (DR) test. The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained (**46**).

Disaster Recovery Plan (DRP)

Limy has developed a disaster recovery plan relying on the AWS platforms which operate according to SOC 2 Type II and ISO 27001:2013 standards. They are designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. It is also designed to sustain the concurrent loss of data in different facilities.

The DRP design allows minimizing service interruption due to hardware failure, natural disaster or a primary data center outage. AWS data centers are organized into Availability Zones (AZ). Each availability zone is comprised of one or more data centers. However, no individual data center can be part of two different AZs. Furthermore, each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located at lower-risk flood plains (specific flood zone categorization varies by region). In addition to a discrete uninterruptible power supply and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers. The Company's production infrastructure is designed with resiliency measures and operational controls to support system availability aligned with business requirements (**45**). The systems are designed to survive temporary or prolonged failure of an availability zone in the event of a disaster. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

Incident Management Process

Limy defines an incident as any irregular or adverse event that impacts the confidentiality, integrity, or availability of company systems, services, or data — including customer or personal data.

Examples of Security Incidents include:

- Loss or theft of equipment containing sensitive data (e.g., laptops, phones)
- Unauthorized access attempts or successful breaches
- Denial-of-Service (DoS) or service outages
- Human error or negligence (e.g., misconfiguration, mishandling credentials)
- Policy or system failures exposing data or weakening controls
- Fraud attempts or insider misuse of systems
- Vendor or service-provider related events compromising confidentiality or availability

Detection and Reporting:
Automated monitoring systems operate 24/7 to detect anomalies and service disruptions.
Employees may manually open incident tickets for events involving:

- Security breaches
- Service availability issues
- Data confidentiality or integrity concerns
- Customer-reported problems
  Customers can report incidents through the support portal, email, chat, or phone. Critical incidents are discussed during periodic risk assessment meetings.

In the event of an outage or a service issue, a notification is sent to the customers. An incident management application is available to Limy's employees in order to report breaches of the system security, availability, confidentiality, and privacy. Customers report issues to their assigned account managers through support application, emails, or phone. Critical incidents are discussed in the risk assessment meetings. Service interruptions are communicated to customers through email notification.

Security Incident Response Policy

The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations (**38**). Whenever a security incident of a physical or electronic nature is suspected or confirmed, all parties covered by this policy are expected to follow appropriate

procedures detailed in this policy. Appropriate compliance and legal personnel are informed of personal data breaches to assist in the response to, and communication of, security incidents internally and externally.
The response process consists of three phases:

1) **Identification**: The security incident is recognized, reported to the Security Response Team (SRT), and confirmed.
2) **Assessment:** The SRT analyzes the security incident and evaluates it for possible causes.
3) **Response:** The SRT responds to each security incident.
4) **Root Cause Analysis (RCA):** Following containment and initial remediation, the SRT conducts a Root Cause Analysis to determine the underlying reasons for the incident and to prevent recurrence.

If any security incident also involves a personal data breach, then the company will also follow the steps which are applicable for such breach (as detailed under "Personal Data Breach").

Risk Assessment

The process of Risk Assessment is a critical component of Limy's internal control system. The purpose of Limy's Risk Assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. As part of the Risk Assessment process, a specific procedure will be taken with regard to identifying, assessing and minimizing privacy risks of projects, systems or policies that involve the collection, use or disclosure of personal data ("Data Protection Impact Assessments", DPIA). The yearly risk assessment report is presented to senior management for review, comment, and approval

Risk Assessment Meeting

Risk assessment meetings are conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. Results are documented. The annual risk assessment report is reviewed and approved by senior management. Risk mitigation activities are performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures are developed and maintained to support these activities (**18**). Environmental, regulatory, and technological changes are monitored, their effects assessed, and their policies updated accordingly. Summarized protocol (MOM) is saved in a dedicated folder and sent by email to relevant managers. Decisions based on the meeting are assigned to resources including a due date for execution and managed through Limy's Change Management application. The DPO communicates the need to promote a DPIA in cases where there is a potentially adverse effect with regard to individuals' privacy rights.

Risk Mitigation

Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity, or the likelihood of the risk occurring and identify the control activities necessary to mitigate the risk. Limy selects and develops control activities that contribute to risk mitigation which achieves the company's acceptable objective levels. The annual risk assessment report is submitted to senior management for their review, feedback, and approval. Also, the risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communication to meet Limy's objectives during response, mitigation, and recovery efforts.

The Management Team considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities. The relevant business processes are thoroughly controlled using a balance of approaches to mitigate risks, considering both manual and automated controls. Financial impacts of the risks are also taken into consideration during the process.

Confidentiality Procedures

Customer confidentiality is of great importance to Limy. As such, Limy has implemented security measures to ensure the confidentiality of its customers' sensitive personal information. Business partners are required to sign agreements containing confidentiality clauses to protect company and customer confidential information (**50**). The security measures aim to prevent unauthorized access, disclosure, alteration, or destruction of sensitive personal information. The Company maintains a Data Retention Policy that outlines procedures for the secure disposal of customer confidential information upon request or in accordance to Company policy. The policy is reviewed and approved on an annual basis (**49**). The Company maintains a documented Information Security Program that defines requirements for protecting the confidentiality, integrity, and availability of systems. Policies are reviewed and approved annually by management (**19**). The Company maintains a vendor management policy that includes vendor termination procedures (**15**).

The company encrypts employees' laptops to safeguard customers' confidentiality. Equipment contacting sensitive information is disposed only after the sensitive information has been wiped out, including revocation of access permissions to the systems and premises, as well as the return of company property and equipment. Customer data at rest is encrypted and hosted separately via secured storage services, provided by AWS. Access to Limy's DB resources, which are located within the production environment, is restricted to authorized personnel. Access to the production environment is restricted to authorized personnel based on job function and least privilege. Access to the AWS management interface is performed using MFA and is restricted to authorized personnel. Encryption between company's customers and the Application is enabled using an authenticated TLS tunnel. Additionally, input and output of customer sessions and transactions are performed using a unique token that is assigned automatically. Finally, a risk assessment meeting is performed on a quarterly basis in order to evaluate risks and threats, and to discuss and address security, confidentiality and availability non-compliance issues. Minutes of the meetings are retained. In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, impacted customers are notified.

Subservice Organization carved-out controls: Amazon Web Services (AWS)

The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment
- Implement logical-access security measures to infrastructure components including native security or security software and appropriate configuration settings
- Restrict access to virtual and physical servers, software, firewalls, and physical storage to authorized individuals
- Review the list of users and permissions on a regular basis
- Implement controls to:
  - Provide access only to authorized people
  - Remove access when no longer appropriate
  - Secure the facilities to permit access only to authorized persons
  - Monitor access to the facilities
- Be consistent with defined system security as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software
- Maintain system components, including configurations consistent with the defined system security, related policies
- Allow only authorized tested and documented changes to be made to the system

Complementary User Entity Controls (CUECs)

The complementary user entity controls are controls that users of Limy need to implement to ensure the secure use of your services. Those are controls that Limy does not take responsibility for. The CUECs are based on control.

	Control Criteria	***User Entities Control Description***
1.	CC6.1, CC6.6	User entities are responsible to take security measures to protect the usernames and passwords of the employees authorized to use the company platform and promptly notify the company if the Company believes its user identification name or password have been used inappropriately or the confidentiality of the information made available through their use has been compromised.
2.	CC6.1, CC6.2, CC6.3	User Entities are responsible to implement controls to ensure that sensitive permissions are reviewed and approved.
3.	CC6.1, CC6.6	User Entities are responsible to implement controls to ensure that MFA configuration is controlled and managed (MFA should not be turned off. If requested, the user entity should treat this user with high security, measurements). The User Entities are responsible to protect the MFA elements properly.
4.	CC6.1, CC6.6	User entities are responsible to implement controls to ensure that personal data is processed legally and not shared with unauthorized third parties.
5.	CC6.1, CC6.2, CC6.3, CC6.6	User entities are responsible to define the list of authorized people in the organization with access to the company and the access levels each person should be granted.
6.	CC6.6, CO1.1, CC7.5	User entities are responsible to notify the company as soon as possible in any case of a breach related to confidential information.
7.	CC4.1, CC4.2, CC7.1	User entities should review reports generated by the company platform for accuracy and completeness.
8.	CC4.1, CC4.2, CC7.1	User entities should: • Implement monitoring procedures to identify and investigate errors and discrepancies in data processed by the company platform. • Educate users on how to identify and report errors and discrepancies in data processed by the company platform. • The User entities should regularly monitor the Logs and events generated by the users to identify abnormal behavior and unauthorized access
9.	CC4.1, CC4.2, CC7.1	User entities should reconcile data processed by the company platform with other systems and data sources on a regular basis.
10.	CC7.4, CC7.5	User entities should develop and implement an incident response plan to respond to security incidents and other disruptions to the company platform. User entities should regularly test the incident response plan to ensure that it is effective.

Section IV - Description of Criteria, Controls, Tests and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by Limy, KFGK considered the aspects of Limy. control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and control

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Limy. The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of tests are the responsibility of the service auditor.

Control Environment

CC1.1 / COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	No deviations noted.
5	All new employees undergo appropriate reference checks as part of the hiring process.	For a sample of new employees, inspected the reference checks documentation and determined that all new employees underwent screening or appropriate reference checks as part of the hiring process.	No deviations noted.
50	Business partners are required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	Inspected a sample of vendors and other third parties' agreement and determined that business partners were required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	No deviations noted.

CC1.2 / COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	Inspected a sample of board meeting minutes and invitations and determined that the board of directors reviewed and approved key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	No deviations noted.

CC1.3 / COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	Inspected a sample of board meeting minutes and invitations and determined that the board of directors reviewed and approved key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	No deviations noted.
3	Company management meets at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	Inspected a sample of management meeting minutes and invitations and determined that company management met at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	No deviations noted.
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	No deviations noted.
9	An organizational chart is maintained and clearly defines management authority and reporting structure.	Inspected company's organizational chart and determined that an organizational chart was maintained and clearly defined management authority and reporting structure.	No deviations noted.

CC1.4 / COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	Job descriptions are documented and are available through the company website.	Inspected a sample of job descriptions and determined that job descriptions were documented and were available through the company website. No job position was opened during the audit period.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
6	New employees complete a formal onboarding process documented through an onboarding checklist, which includes required steps such as the receipt of company-issued equipment (e.g., a laptop).	For a sample of new employees, inspected the onboarding documentation performed and determined that new employees completed a formal onboarding process documented through an onboarding checklist, which included required steps such as the receipt of company-issued equipment (e.g., a laptop).	No deviations noted.
7	Professional training is provided based on development needs or operational demands. Training materials, guidelines, and relevant documentation are made available through the company's knowledge management portal.	For a sample of R&D employees, inspected the training documentation and the meeting minutes and attendance certificates and determined that professional training was provided based on development needs or operational demands. Training materials, guidelines, and relevant documentation were made available through the company's knowledge management portal.	No deviations noted.
8	All employees receive annual security awareness training and are required to acknowledge completion.	For a sample of current employees, inspected the training quiz and examination certificates and determined that all employees received annual security awareness training and were required to acknowledge completion.	No deviations noted.
19	The Company maintains a documented Information Security Program that defines requirements for protecting the confidentiality, integrity, and availability of systems. Policies are reviewed and approved annually by management.	Inspected the information security policy and determined that the company maintained a documented information security program that defined requirements for protecting the confidentiality, integrity, and availability of systems. Policies were reviewed and approved annually by management.	No deviations noted.

CC1.5 / COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	annually and are available to all employees via the company's internal portal.	basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	
6	New employees complete a formal onboarding process documented through an onboarding checklist, which includes required steps such as the receipt of company-issued equipment (e.g., a laptop).	For a sample of new employees, inspected the onboarding documentation performed and determined that new employees completed a formal onboarding process documented through an onboarding checklist, which included required steps such as the receipt of company-issued equipment (e.g., a laptop).	No deviations noted.
7	Professional training is provided based on development needs or operational demands. Training materials, guidelines, and relevant documentation are made available through the company's knowledge management portal.	For a sample of R&D employees, inspected the training documentation and the meeting minutes and attendance certificates and determined that professional training was provided based on development needs or operational demands. Training materials, guidelines, and relevant documentation were made available through the company's knowledge management portal.	No deviations noted.
10	Employees are subject to a periodic feedback process.	For a sample of current employees, inspected the feedback documentation and determined that employees were subject to a periodic feedback process.	No deviations noted.

Communication and Information

CC2.1 / COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

CC2.2 / COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	No deviations noted.
6	New employees complete a formal onboarding process documented through an onboarding checklist, which includes required steps such as the receipt of company-issued equipment (e.g., a laptop).	For a sample of new employees, inspected the onboarding documentation performed and determined that new employees completed a formal onboarding process documented through an onboarding checklist, which included required steps such as the receipt of company-issued equipment (e.g., a laptop).	No deviations noted.
8	All employees receive annual security awareness training and are required to acknowledge completion.	For a sample of current employees, inspected the training quiz and examination certificates and determined that all employees received annual security awareness training and were required to acknowledge completion.	No deviations noted.
19	The Company maintains a documented Information Security Program that defines requirements for protecting the confidentiality, integrity, and availability of systems. Policies are reviewed and approved annually by management.	Inspected the information security policy and determined that the company maintained a documented information security program that defined requirements for protecting the confidentiality, integrity, and availability of systems. Policies were reviewed and approved annually by management.	No deviations noted.
38	The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy	Inspected the security incident response management policy and determined that the company had developed and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations. No incidents were identified during the audit period.	

CC2.3 / COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	The Company provides customer-facing "How-To" guidance through the website.	Inspected the How-To section and determined that the company provided customer-facing "how-to" guidance through the website-designated customer communication channels.	No deviations noted.
13	Significant new features are communicated to customers through designated communication channels in accordance with the company's communication procedures.	Inspected a sample of release notes and determined that significant new features were communicated to customers through designated communication channels in accordance with the company's communication procedures.	No deviations noted.
14	A dedicated communication channel is available to customers.	Inspected the internal portal and determined that a dedicated communication channel was available to customers.	No deviations noted.
38	The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	Inspected the security incident response management policy and determined that the company had developed and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		regulatory obligations. No incidents were identified during the audit period.	
42	The Company monitors system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications are communicated to customers based on management's determination.	Inspected the Uptime report and determined that the company monitored system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications were communicated to customers based on management's determination. There was no communication of downtime during the audit period.	No deviations noted.

Risk Assessment

CC3.1 / COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
18	Risk assessment meetings are conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. Results are documented. The annual risk assessment report is reviewed and approved by senior management. Risk mitigation activities are performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures are developed and maintained to support these activities.	Inspected a sample of risk assessment meeting minutes and invitations and determined that that risk assessment meetings were conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. results were documented. Inspected the risk mitigation plan documentation and determined that the annual risk assessment report was reviewed and approved by senior management. Risk mitigation activities were performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures were developed and maintained to support these activities.	No deviations noted.
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

CC3.2 / COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	Inspected a sample of board meeting minutes and invitations and determined that the board of directors reviewed and approved key operational, strategic, strategic, strategic, governance, and risk-related matters at least annually via written board resolutions.	No deviations noted.
3	Company management meets at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	Inspected a sample of management meeting minutes and invitations and determined that company management met at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	No deviations noted.
18	Risk assessment meetings are conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. Results are documented. The annual risk assessment report is reviewed and approved by senior management. Risk mitigation activities are performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures are developed and maintained to support these activities.	Inspected a sample of risk assessment meeting minutes and invitations and determined that that risk assessment meetings were conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. results were documented. Inspected the risk mitigation plan documentation and determined that the annual risk assessment report was reviewed and approved by senior management. Risk mitigation activities were performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures were developed and maintained to support these activities.	No deviations noted.
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

CC3.3 / COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	Inspected a sample of board meeting minutes and invitations and determined that the board of directors reviewed and approved key operational, strategic, strategic, governance, and risk-related matters at least annually via written board resolutions.	No deviations noted.
3	Company management meets at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	Inspected a sample of management meeting minutes and invitations and determined that company management met at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	No deviations noted.
18	Risk assessment meetings are conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. Results are documented. The annual risk assessment report is reviewed and approved by senior management. Risk mitigation activities are performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures are developed and maintained to support these activities.	Inspected a sample of risk assessment meeting minutes and invitations and determined that that risk assessment meetings were conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. results were documented. Inspected the risk mitigation plan documentation and determined that the annual risk assessment report was reviewed and approved by senior management. Risk mitigation activities were performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures were developed and maintained to support these activities.	No deviations noted.
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

CC3.4 / COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	The Company maintains a vendor management policy that includes vendor termination procedures.	Inspected the vendor management policy and determined that the company maintained a vendor management policy that included vendor termination procedures. The policy was reviewed and approved at least annually.	No deviations noted.
34	Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	Inspected the Internal vulnerability scan report and determined that vulnerability assessments were conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	No deviations noted.
35	Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline.	Inspected a sample of vulnerability scan reports and determined that vulnerability scans were performed on production-related code using a specialized tool and were integrated into the SDLC pipeline. Inspected examples of vulnerability alerts and tickets and determined that they were tracked until resolution.	No deviations noted.
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

Monitoring Activities

CC4.1 / COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	The Company maintains a documented Information Security Program that defines requirements for protecting the confidentiality, integrity, and	Inspected the information security policy and determined that the company maintained a documented information security program that defined requirements for protecting the confidentiality,	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	availability of systems. Policies are reviewed and approved annually by management.	integrity, and availability of systems. Policies were reviewed and approved annually by management.	
32	Operational activities within the production environment are monitored and logged. Logs are reviewed by a designated team, and alerts are generated upon detection of anomalous activity.	Inspected the production monitoring logs and alerts and determined that operational activities within the production environment were monitored and logged. Logs were reviewed by a designated team, and alerts were generated upon detection of anomalous activity.	No deviations noted.
37	Intrusion detection systems are used to provide continuous monitoring of the company's network and to detect potential security breaches.	Inspected the AWS monitoring dashboard and determined that intrusion detection systems were used to provide continuous monitoring of the company's network and to detect potential security breaches.	No deviations noted.
42	The Company monitors system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications are communicated to customers based on management's determination.	Inspected the Uptime report and determined that the company monitored system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications were communicated to customers based on management's determination. There was no downtime communicated during the audit period.	No deviations noted.
43	Uptime commitments to customers are defined in the applicable SLA agreements.	Inspected the internal SLA and determined that uptime commitments to customers were defined in the applicable SLA agreements.	No deviations noted.

CC4.2 / COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
37	Intrusion detection systems are used to provide continuous monitoring of the company's network and to detect potential security breaches.	Inspected the AWS monitoring dashboard and determined that intrusion detection systems were used to provide continuous monitoring of the company's network and to detect potential security breaches.	No deviations noted.
38	The Company has developed and maintains a Security Incident Response Policy designed to	Inspected the security incident response management policy and determined that the company had developed	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations. No incidents were identified during the audit period.	
42	The Company monitors system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications are communicated to customers based on management's determination.	Inspected the Uptime report and determined that the company monitored system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications were communicated to customers based on management's determination. There was no downtime communicated during the audit period.	No deviations noted.
43	Uptime commitments to customers are defined in the applicable SLA agreements.	Inspected the internal SLA and determined that uptime commitments to customers were defined in the applicable SLA agreements.	No deviations noted.

Control Activities

CC5.1 / COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

CC5.2 / COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
8	All employees receive annual security awareness training and are required to acknowledge completion.	For a sample of current employees, inspected the training quiz and examination certificates and determined that all employees received annual security awareness training and were required to acknowledge completion.	No deviations noted.
19	The Company maintains a documented Information Security Program that defines requirements for protecting the confidentiality, integrity, and availability of systems. Policies are reviewed and approved annually by management.	Inspected the information security policy and determined that the company maintained a documented information security program that defined requirements for protecting the confidentiality, integrity, and availability of systems. Policies were reviewed and approved annually by management.	No deviations noted.

CC5.3 / COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company’s internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	No deviations noted.
15	The Company maintains a vendor management policy that includes vendor termination procedures.	Inspected the vendor management policy and determined that the company maintained a vendor management policy that included vendor termination procedures. The policy was reviewed and approved at least annually.	No deviations noted.
19	The Company maintains a documented Information Security Program that defines requirements for protecting the confidentiality, integrity, and	Inspected the information security policy and determined that the company maintained a documented information security program that defined requirements for protecting the confidentiality,	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	availability of systems. Policies are reviewed and approved annually by management.	integrity, and availability of systems. Policies were reviewed and approved annually by management.	
39	The Company maintains a documented Change Management Policy, which is reviewed and approved at least annually.	Inspected the Change Management Policy and determined that the company maintained a documented change management policy, which was reviewed and approved at least annually.	No deviations noted.

Logical and Physical Access Controls

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	The Company maintains an architecture diagram that illustrates system components and security and protection measures for system resources.	Inspected the architecture diagram and determined that the company maintained an architecture diagram that illustrated system components and security and protection measures for system resources.	No deviations noted.
20	Security practices enforce logical separation between different environments, such as Development, Testing, Staging, and Production.	Inspected the cloud provider and determined that security practices enforced logical separation between different environments, such as development, testing, staging, and production.	No deviations noted.
22	Users are authenticated using unique user IDs and passwords via an Identity Provider (SSO) and/or directly within systems. Passwords are configured to meet defined security requirements.	Inspected the password configuration settings and determined that users were authenticated using unique user ids and passwords via an identity provider (sso) and/or directly within systems. Passwords were configured to meet defined security requirements. Inspected the applications linked to the SSO tool and determined that AWS was linked to the SSO.	No deviations noted.
23	Access to the AWS production environment requires Multi-Factor Authentication (MFA) and is restricted to authorized users.	Inspected the list of users with access to the production environment and determined that it was restricted to authorized users. Inspected the MFA configuration and determined that it required two-factor authentication.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
25	Access to source code repositories requires MFA and is restricted to authorized users. Also, access to modify branch configuration within the source code management tool is restricted to authorized users to ensure proper segregation of duties.	Inspected the list of users with access to the source code and determined that access to source code repositories required MFA and was restricted to authorized users. Also, access to modify branch configuration within the source code management tool was restricted to authorized users to ensure proper segregation of duties.	No deviations noted.
26	Access to build tools requires MFA and is restricted to authorized users.	Inspected the list of users with access to the build tools and determined that it was restricted to authorized personnel. Inspected the two-factor configuration and determined that it required two-factor authentication.	No deviations noted.
28	Firewalls are configured to restrict unnecessary ports, protocols, and services.	Inspected the firewall rules configuration and determined that firewalls were configured to restrict unnecessary ports, protocols, and services.	No deviations noted.
48	Customer data at rest is encrypted and hosted in secured storage services.	Inspected the database encryption configuration and determined that customer data at rest was encrypted and hosted in secured storage services.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
6	New employees complete a formal onboarding process documented through an onboarding checklist, which includes required steps such as the receipt of company-issued equipment (e.g., a laptop).	For a sample of new employees, inspected the onboarding documentation performed and determined that new employees completed a formal onboarding process documented through an onboarding checklist, which included required steps such as the receipt of company-issued equipment (e.g., a laptop).	No deviations noted.
21	New employees are granted access to the different environments upon job requirements based on the employee permission table.	Inspected the employee permission table and the user provisioning audit logs and determined that new employees were granted access to the different	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		environments upon job requirements based on the employee permission table.	
27	Permissions to production-related systems are reviewed, approved, and documented by Company management at least annually.	Inspected the user access review documentation and determined that permissions to production-related systems were reviewed, approved, and documented by company management at least annually.	No deviations noted.
31	Access to production-related systems is revoked upon employee termination. Company-issued equipment is returned in a timely manner, as documented in the offboarding checklists.	For a sample of terminated employees, inspected the offboarding checklist and determined that access to production-related systems was revoked upon employee termination. company-issued equipment was returned in a timely manner, as documented in the offboarding checklists.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	No deviations noted.
27	Permissions to production-related systems are reviewed, approved, and documented by Company management at least annually.	Inspected the user access review documentation and determined that permissions to production-related systems were reviewed, approved, and documented by company management at least annually.	No deviations noted.
31	Access to production-related systems is revoked upon employee termination. Company-issued equipment is returned in a timely manner, as documented in the offboarding checklists.	For a sample of terminated employees, inspected the offboarding checklist and determined that access to production-related systems was revoked upon employee termination. company-issued equipment was	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		returned in a timely manner, as documented in the offboarding checklists.	

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures were available to the company's employees within the company internal portal.	No deviations noted.
29	Physical access to company offices is restricted to authorized personnel through a designated access control system. Access is granted to company employees only, and all visitors are required to be escorted by a company employee at all times while on the premises.	Inspected the Security and Architecture Policy and determined that physical access to company offices was restricted to authorized personnel through a designated access control system. Access was granted to company employees only, and all visitors were required to be escorted by a company employee at all times while on the premises.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
29	Physical access to company offices is restricted to authorized personnel through a designated access control system. Access is granted to company employees only, and all visitors are required to be escorted by a company employee at all times while on the premises.	Inspected the Security and Architecture Policy and determined that physical access to company offices was restricted to authorized personnel through a designated access control system. Access was granted to company employees only, and all visitors were required to be escorted by a company employee at all times while on the premises.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	Inspected a sample of board meeting minutes and invitations and determined that the board of directors reviewed and approved key operational, strategic, strategic, governance, and risk-related matters at least annually via written board resolutions.	No deviations noted.
20	Security practices enforce logical separation between different environments, such as Development, Testing, Staging, and Production.	Inspected the cloud provider and determined that security practices enforced logical separation between different environments, such as development, testing, staging, and production.	No deviations noted.
33	An antivirus solution is installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software.	For a sample of current employees, inspected the updated antivirus status and determined that an antivirus solution was installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software. Employees' laptops were encrypted to safeguard the confidentiality of customer data.	No deviations noted.
47	Data transmitted between the company's customers and the application is encrypted using an authenticated TLS tunnel.	Inspected the TLS configuration and determined that data transmitted between the company's customers and the application was encrypted using an authenticated TLS tunnel.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
33	An antivirus solution is installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software.	For a sample of current employees, inspected the updated antivirus status and determined that an antivirus solution was installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software. Employees' laptops	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		were encrypted to safeguard the confidentiality of customer data.	

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	The Company conducts an annual review of the data center vendor's SOC2 report. Any identified deviations are reviewed and investigated as appropriate. The review includes identifying and documenting the controls implemented by the Company to address applicable Complementary User Entity Controls (CUECs).	Inspected the review of the AWS data center SOC 2 report and determined that the company conducted an annual review of the data center vendor's soc 2 report. Any identified deviations were reviewed and investigated as appropriate. The review included identifying and documenting the controls implemented by the company to address applicable complementary user entity controls (cuecs).	No deviations noted.
33	An antivirus solution is installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software.	For a sample of current employees, inspected the updated antivirus status and determined that an antivirus solution was installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software. Employees' laptops were encrypted to safeguard the confidentiality of customer data.	No deviations noted.
34	Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	Inspected the Internal vulnerability scan report and determined that vulnerability assessments were conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	No deviations noted.
35	Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline.	Inspected a sample of vulnerability scan reports and determined that vulnerability scans were performed on production-related code using a specialized tool and were integrated into the sdlc pipeline. Inspected examples of vulnerability alerts and tickets and determined that they were tracked until resolution.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
36	A penetration test is performed at least annually. Any identified high-severity findings are investigated and remediated through the SDLC process or other appropriate measures.	Inspected the penetration test report and determined that a penetration test was performed at least annually. Any identified high-severity findings were investigated and remediated through the SDLC process or other appropriate measures.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
34	Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	Inspected the Internal vulnerability scan report and determined that vulnerability assessments were conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	No deviations noted.
35	Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline.	Inspected a sample of vulnerability scan reports and determined that vulnerability scans were performed on production-related code using a specialized tool and were integrated into the SDLC pipeline. Inspected examples of vulnerability alerts and tickets and determined that they were tracked until resolution.	No deviations noted.
36	A penetration test is performed at least annually. Any identified high-severity findings are investigated and remediated through the SDLC process or other appropriate measures.	Inspected the penetration test report and determined that a penetration test was performed at least annually. Any identified high-severity findings were investigated and remediated through the SDLC process or other appropriate measures.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
33	An antivirus solution is installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software.	For a sample of current employees, inspected the updated antivirus status and determined that an antivirus solution was installed on employees' laptops to detect and prevent the installation or spread of unauthorized or malicious software. Employees' laptops were encrypted to safeguard the confidentiality of customer data.	No deviations noted.
36	A penetration test is performed at least annually. Any identified high-severity findings are investigated and remediated through the SDLC process or other appropriate measures.	Inspected the penetration test report and determined that a penetration test was performed at least annually. Any identified high-severity findings were investigated and remediated through the sdlc process or other appropriate measures.	No deviations noted.
37	Intrusion detection systems are used to provide continuous monitoring of the company's network and to detect potential security breaches.	Inspected the AWS monitoring dashboard and determined that intrusion detection systems were used to provide continuous monitoring of the company's network and to detect potential security breaches.	No deviations noted.

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
34	Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	Inspected the Internal vulnerability scan report and determined that vulnerability assessments were conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	No deviations noted.
35	Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline.	Inspected a sample of vulnerability scan reports and determined that vulnerability scans were performed on production-related code using a specialized tool and were integrated into the SDLC pipeline. Inspected	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		examples of vulnerability alerts and tickets and determined that they were tracked until resolution.	
37	Intrusion detection systems are used to provide continuous monitoring of the company's network and to detect potential security breaches.	Inspected the AWS monitoring dashboard and determined that intrusion detection systems were used to provide continuous monitoring of the company's network and to detect potential security breaches.	No deviations noted.
38	The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	Inspected the security incident response management policy and determined that the company had developed and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations. No incidents were identified during the audit period.	No deviations noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
34	Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	Inspected the Internal vulnerability scan report and determined that vulnerability assessments were conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	No deviations noted.
35	Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline.	Inspected a sample of vulnerability scan reports and determined that vulnerability scans were performed on production-related code using a specialized tool and were integrated into the SDLC pipeline. Inspected	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		examples of vulnerability alerts and tickets and determined that they were tracked until resolution.	
38	The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	Inspected the security incident response management policy and determined that the company had developed and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations. No incidents were identified during the audit period.	No deviations noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	The Company maintains a vendor management policy that includes vendor termination procedures.	Inspected the vendor management policy and determined that the company maintained a vendor management policy that included vendor termination procedures. The policy was reviewed and approved at least annually.	No deviations noted.
34	Vulnerability assessments are conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	Inspected the Internal vulnerability scan report and determined that vulnerability assessments were conducted on a continuous basis across the production environment, infrastructure, and network to identify potential security risks.	No deviations noted.
35	Vulnerability scans are performed on production-related code using a specialized tool and are integrated into the SDLC pipeline.	Inspected a sample of vulnerability scan reports and determined that vulnerability scans were performed on production-related code using a specialized tool and were integrated into the SDLC pipeline. Inspected	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		examples of vulnerability alerts and tickets and determined that they were tracked until resolution.	
38	The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	Inspected the security incident response management policy and determined that the company had developed and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations. No incidents were identified during the audit period.	No deviations noted.
42	The Company monitors system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications are communicated to customers based on management's determination.	Inspected the Uptime report and determined that the company monitored system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications were communicated to customers based on management's determination. There was no communicated downtime during the audit period.	No deviations noted.

Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
25	Access to source code repositories requires MFA and is restricted to authorized users. Also, access to modify branch configuration within the source code management tool is restricted to authorized users to ensure proper segregation of duties.	Inspected the list of users with access to the source code and determined that access to source code repositories required MFA and was restricted to authorized users. Also, access to modify branch configuration within the source code management tool	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		was restricted to authorized users to ensure proper segregation of duties.	
26	Access to build tools requires MFA and is restricted to authorized users.	Inspected the list of users with access to the build tools and determined that it was restricted to authorized personnel. Inspected the two-factor configuration and determined that it required two-factor authentication.	No deviations noted.
39	The Company maintains a documented Change Management Policy, which is reviewed and approved at least annually.	Inspected the Change Management Policy and determined that the company maintained a documented change management policy, which was reviewed and approved at least annually.	No deviations noted.
40	Design, implementation, configuration, modification, and management of infrastructure and software are documented and approved through the change management application. Change management tickets are prioritized and labeled based on development phase and urgency. Infrastructure changes follow the same process as code changes. Automated tests are performed using a designated tool to validate code quality. Code review is mandatory as part of the SDLC and is documented within the source control system. Successful completion of required tests is mandatory before continuing the SDLC process and deploying changes to the production environment. Change management tickets are linked to the source control system to associate each request with the corresponding code change.	For a sample of Code and Infrastructure changes, inspected the linked change management tickets and determined that design, implementation, configuration, modification, and management of infrastructure and software were documented and approved through the change management application. Change management tickets were linked to the source control system to associate each request with the corresponding code change. Infrastructure changes followed the same process as code changes. For a sample of Code and Infrastructure changes, inspected the documented code reviews and determined that code review was mandatory as part of the SDLC and was recorded within the source control system. For a sample of Code and Infrastructure changes, inspected the automated tests and determined that automated tests were performed using a designated tool to validate code quality. Successful completion of the required tests was mandatory before continuing the	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		SDLC process and deploying changes to the production environment. Inspected the branch configuration and determined that successful completion of the required tests was mandatory before continuing the SDLC process and deploying changes to the production environment.	

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	The Company conducts annual evaluations of vendors and suppliers to confirm that their controls align with company policies and requirements.	Inspected vendor mapping and determined that the company conducted annual evaluations of vendors and suppliers to confirm that their controls aligned with company policies and requirements.	No deviations noted.
38	The Company has developed and maintains a Security Incident Response Policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy includes procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations.	Inspected the security incident response management policy and determined that the company had developed and maintained a security incident response policy designed to effectively identify, respond to, and manage security incidents and personal data breaches in accordance with applicable laws and regulations. The policy included procedures for timely notification of affected data subjects, regulators, and other relevant parties, as required, to meet the company's privacy and regulatory obligations. No incidents were identified during the audit period.	No deviations noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	In accordance with company policies, all new hires are required to sign a standard employment	For a sample of new employees, inspected the signed NDAs and determined that in accordance with company	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	agreement that outlines confidentiality, Information Protection Awareness, and intellectual property clauses.	policies, all new hires were required to sign a standard employment agreement that outlined confidentiality, information protection awareness, and intellectual property clauses.	
2	The Board of Directors reviews and approves key operational, strategic, governance, and risk-related matters at least annually via written board resolutions.	Inspected a sample of board meeting minutes and invitations and determined that the board of directors reviewed and approved key operational, strategic, strategic, governance, and risk-related matters at least annually via written board resolutions.	No deviations noted.
3	Company management meets at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	Inspected a sample of management meeting minutes and invitations and determined that company management met at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	No deviations noted.
18	Risk assessment meetings are conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. Results are documented. The annual risk assessment report is reviewed and approved by senior management. Risk mitigation activities are performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures are developed and maintained to support these activities.	Inspected a sample of risk assessment meeting minutes and invitations and determined that that risk assessment meetings were conducted at least annually to identify, analyze, and respond to risks related to security, availability, confidentiality, and compliance. results were documented. Inspected the risk mitigation plan documentation and determined that the annual risk assessment report was reviewed and approved by senior management. Risk mitigation activities were performed to respond to, reduce, and recover from security events that could disrupt business operations. Policies and procedures were developed and maintained to support these activities.	No deviations noted.
30	The Company conducts an annual review of the data center vendor's SOC2 report. Any identified deviations are reviewed and investigated as appropriate. The review includes identifying and	Inspected the review of the AWS data center SOC 2 report and determined that the company conducted an annual review of the data center vendor's soc 2 report. Any identified deviations were reviewed and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	documenting the controls implemented by the Company to address applicable Complementary User Entity Controls (CUECs).	investigated as appropriate. The review included identifying and documenting the controls implemented by the company to address applicable complementary user entity controls (CUECS).	
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.
50	Business partners are required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	Inspected a sample of vendors and other third parties' agreement and determined that business partners were required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	No deviations noted.

Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
42	The Company monitors system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications are communicated to customers based on management’s determination.	Inspected the Uptime report and determined that the company monitored system uptime to help ensure the availability and reliability of its services. Service interruption and maintenance notifications were communicated to customers based on management’s determination. There was no downtime communicated during the audit period.	No deviations noted.
43	Uptime commitments to customers are defined in the applicable SLA agreements.	Inspected the internal SLA and determined that uptime commitments to customers were defined in the applicable sla agreements.	No deviations noted.
44	The Company performs backups of its application database to support data availability and recovery.	Inspected the backup system configuration and the backup logs and determined that the company	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		performed backups of its application database to support data availability and recovery.	
45	The Company's production infrastructure is designed with resiliency measures and operational controls to support system availability aligned with business requirements.	Inspected the AWS availability zones configuration and determined that the company's production infrastructure was designed with resiliency measures and operational controls to support system availability aligned with business requirements.	No deviations noted.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
44	The Company performs backups of its application database to support data availability and recovery.	Inspected the backup system configuration and the backup logs and determined that the company performed backups of its application database to support data availability and recovery.	No deviations noted.
45	The Company's production infrastructure is designed with resiliency measures and operational controls to support system availability aligned with business requirements.	Inspected the AWS availability zones configuration and determined that the company's production infrastructure was designed with resiliency measures and operational controls to support system availability aligned with business requirements.	No deviations noted.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	The Company maintains a vendor management policy that includes vendor termination procedures.	Inspected the vendor management policy and determined that the company maintained a vendor management policy that included vendor termination procedures. The policy was reviewed and approved at least annually.	No deviations noted.
16	The Company conducts annual evaluations of vendors and suppliers to confirm that their controls align with company policies and requirements.	Inspected vendor mapping and determined that the company conducted annual evaluations of vendors and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		suppliers to confirm that their controls aligned with company policies and requirements.	
46	The Company performs restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process is documented and retained.	Inspected the Disaster Recovery policy and the DR drill document and determined that the company performed restore tests at least annually to validate disaster recovery capabilities. The disaster recovery process was documented and retained.	No deviations noted.

Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	In accordance with company policies, all new hires are required to sign a standard employment agreement that outlines confidentiality, Information Protection Awareness, and intellectual property clauses.	For a sample of new employees, inspected the signed NDAs and determined that in accordance with company policies, all new hires were required to sign a standard employment agreement that outlined confidentiality, information protection awareness, and intellectual property clauses.	No deviations noted.
3	Company management meets at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	Inspected a sample of management meeting minutes and invitations and determined that company management met at least on a monthly basis to discuss ongoing operational matters, risks, and organizational updates.	No deviations noted.
22	Users are authenticated using unique user IDs and passwords via an Identity Provider (SSO) and/or directly within systems. Passwords are configured to meet defined security requirements.	Inspected the password configuration settings and determined that users were authenticated using unique user ids and passwords via an identity provider (SSO) and/or directly within systems. Passwords were configured to meet defined security requirements. Inspected the applications linked to the SSO tool and determined that AWS was linked to the SSO.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
23	Access to the AWS production environment requires Multi-Factor Authentication (MFA) and is restricted to authorized users.	Inspected the list of users with access to the production environment and determined that it was restricted to authorized users. Inspected the MFA configuration and determined that it required two-factor authentication.	No deviations noted.
47	Data transmitted between the company's customers and the application is encrypted using an authenticated TLS tunnel.	Inspected the TLS configuration and determined that data transmitted between the company's customers and the application was encrypted using an authenticated TLS tunnel.	No deviations noted.
48	Customer data at rest is encrypted and hosted in secured storage services.	Inspected the database encryption configuration and determined that customer data at rest was encrypted and hosted in secured storage services.	No deviations noted.
49	The Company maintains a Data Retention Policy that outlines procedures for the secure disposal of customer confidential information upon request or in accordance to company policy. The policy is reviewed and approved on an annual basis.	Inspected the Data Retention Policy and determined that the company maintained a data retention policy that outlined procedures for the secure disposal of customer confidential information upon request or in accordance with company policy. The policy was reviewed and approved on an annual basis.	No deviations noted.
50	Business partners are required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	Inspected a sample of vendors and other third parties' agreement and determined that business partners were required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	No deviations noted.

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are formally documented, reviewed, and approved by Management at least annually and are available to all employees via the company's internal portal.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team. Inspected the internal portal and determined that policies and procedures	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		were available to the company's employees within the company internal portal.	
23	Access to the AWS production environment requires Multi-Factor Authentication (MFA) and is restricted to authorized users.	Inspected the list of users with access to the production environment and determined that it was restricted to authorized users. Inspected the MFA configuration and determined that it required two-factor authentication.	No deviations noted.
49	The Company maintains a Data Retention Policy that outlines procedures for the secure disposal of customer confidential information upon request or in accordance to company policy. The policy is reviewed and approved on an annual basis.	Inspected the Data Retention Policy and determined that the company maintained a data retention policy that outlined procedures for the secure disposal of customer confidential information upon request or in accordance with company policy. The policy was reviewed and approved on an annual basis.	No deviations noted.
50	Business partners are required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	Inspected a sample of vendors and other third parties' agreement and determined that business partners were required to sign agreements containing confidentiality clauses to protect company and customer confidential information.	No deviations noted.

****