ILLUSTRATIVE SAMPLE

Sablewick, Inc. is a fictitious company. This is not an issued report.

SYSTEM AND ORGANIZATION CONTROLS (SOC) 2 · TYPE II REPORT

Sablewick

the service organization's logo appears here

Report on the Sablewick Platform System

Relevant to the Trust Services Criteria for Security and Availability

SERVICE ORGANIZATION	EXAMINATION PERIOD	SERVICE AUDITOR
SABLEWICK, INC.	**July 1, 2025 to June 30, 2026**	**Y Assurance PLLC**

CONFIDENTIAL

Prepared July 2026

Contents

About this sample

This document is an ILLUSTRATIVE SAMPLE produced by Y Assurance PLLC to show the form and content of a SOC 2 Type II report. It is not an issued report.

Sablewick, Inc. is a fictitious company. It does not exist. Every person, system, date, population, test result and management response in this document is invented for illustration. No examination was performed, no opinion is expressed, and nothing here describes any real organization.

The control set, the control descriptions and the trust services criteria shown are the real ones Y Assurance PLLC uses, so the sample reflects the methodology actually applied on an engagement. What is invented is the company and its results, not the method.

The firm's signature is deliberately withheld. A signature is one person putting their name to a specific examination, and no examination happened here. On an issued report it appears at the end of Section 1.

The AICPA SOC logo on the cover marks Y Assurance PLLC as a licensed CPA firm permitted to perform SOC engagements. It says nothing about Sablewick, Inc. and it is not an endorsement of this document by the AICPA.

SECTION 1

Independent Service Auditor's Report

Y Assurance

Y Assurance PLLC
Texas Firm Registration C12398
5900 Balcones Dr
Austin, TX 78731

July 14, 2026

To the Management of Sablewick, Inc.:

INDEPENDENT SERVICE AUDITOR'S REPORT

Scope

We have examined Sablewick's accompanying description of its Sablewick Platform system titled "Sablewick's Description of Its Sablewick Platform System Throughout the Period July 1, 2025 to June 30, 2026" (description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance – 2022) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Sablewick's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022).

Sablewick uses Amazon Web Services (AWS) (the subservice organization) to provide cloud hosting services for the production environment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sablewick, to achieve Sablewick's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Sablewick's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Sablewick, to achieve Sablewick's service commitments and system requirements based on the applicable trust services criteria. 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 controls.

The information included in Section 5, "Other Information Provided by Sablewick That Is Not Covered by the Service Auditor's Report," is presented by Sablewick management to provide additional information and is not a part of Sablewick's description of its Sablewick Platform system made available to user entities during the period July 1, 2025 to June 30, 2026. Information included in Sablewick's responses to testing exceptions

has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

Sablewick 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. Sablewick has provided the accompanying assertion titled "Assertion of Sablewick Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Sablewick is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we 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 the following:

- 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 the controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of the controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements 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. The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 of this report.

Service Auditor's Independence and Quality Management

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We apply the Statements on Quality Management Standards established by the AICPA and, accordingly, maintain a system of quality management, including policies and procedures addressing compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

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 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 prevent, or detect and correct, all misstatements or events relevant to the applicable trust services criteria. The projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

a. the description presents Sablewick's Sablewick Platform system that was designed and implemented throughout the period July 1, 2025 to June 30, 2026 in accordance with the description criteria, and

b. the controls stated in the description were suitably designed throughout the period July 1, 2025 to June 30, 2026 to provide reasonable assurance that Sablewick's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if user entities applied the complementary user entity controls and the subservice organization applied the complementary subservice organization controls assumed in the design of Sablewick's controls throughout that period, and

c. the controls stated in the description operated effectively throughout the period July 1, 2025 to June 30, 2026 to provide reasonable assurance that Sablewick's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Sablewick's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Sablewick; user entities of Sablewick's Sablewick Platform system during some or all of the period July 1, 2025 to June 30, 2026; business partners of Sablewick subject to risks arising from interactions with the Sablewick Platform system; prospective user entities and business partners; regulators; and practitioners providing services to such user entities and business partners who have sufficient knowledge and understanding of the nature of the services provided by the service organization; how the service organization's system interacts with user entities and other parties; internal control and its limitations; the applicable trust services criteria; and 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.

If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the nonspecified user's sole responsibility and at the nonspecified user's sole and exclusive risk. Nonspecified users may not rely on this report and do not acquire any rights against Y Assurance PLLC as a result of such access. Y Assurance PLLC does not assume any duties or obligations to any nonspecified user who obtains this report or has access to it.

Sincerely,

[firm signature withheld: illustrative sample]

Y Assurance PLLC

Austin, Texas

July 14, 2026

SECTION 2

Assertion of Sablewick Management

ASSERTION OF SABLEWICK MANAGEMENT

We have prepared the accompanying description of Sablewick's Sablewick Platform system titled "Sablewick's Description of Its Sablewick Platform System Throughout the Period July 1, 2025 to June 30, 2026" (description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance – 2022) (description criteria). The description is intended to provide report users with information about the Sablewick Platform system that may be useful when assessing the risks arising from interactions with Sablewick's system throughout the period July 1, 2025 to June 30, 2026, particularly information about system controls that Sablewick 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 and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022).

Sablewick uses Amazon Web Services (AWS) (the subservice organization) to provide cloud hosting services for the production environment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sablewick, to achieve Sablewick's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Sablewick's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Sablewick, to achieve Sablewick's service commitments and system requirements based on the applicable trust services criteria.

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

a. the description presents Sablewick's Sablewick Platform system that was designed and implemented throughout the period July 1, 2025 to June 30, 2026 in accordance with the description criteria, and

b. the controls stated in the description were suitably designed throughout the period July 1, 2025 to June 30, 2026 to provide reasonable assurance that Sablewick's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if user entities applied the complementary user entity controls and the subservice organization applied the complementary subservice organization controls assumed in the design of Sablewick's controls throughout that period, and

c. the controls stated in the description operated effectively throughout the period July 1, 2025 to June 30, 2026 to provide reasonable assurance that Sablewick's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Sablewick's controls operated effectively throughout that period.

_____

Marisol Trent

Chief Executive Officer

Sablewick, Inc.

Date: _____

SECTION 3

Sablewick's Description of Its Sablewick Platform System Throughout the Period July 1, 2025 to June 30, 2026

Company Overview and Services Provided

Sablewick, Inc. is a Delaware corporation founded in March 2024 and operated by its two founders. Sablewick operates the Sablewick Platform, an evaluation and observability service for teams running large language model applications in production. Customers send prompt and response traces from their own applications to the platform through an API or a client library; the platform stores those traces, scores them against evaluation criteria the customer configures, and reports on output quality and regressions through a web application that customers reach after authentication.

The company operates fully remotely and holds no offices, data centers or server rooms. Its two founders are the only employees: one is responsible for the security program, vendor management and customer commitments, and the other is the only person who writes and deploys production code and administers the cloud account. Two contractors were engaged during the period for defined pieces of work, neither of whom held access to production infrastructure. Oversight of the security program is exercised by the founders together with an outside technical advisor and the lead seed investor, who receive a written security and compliance update each quarter and hold no operational role in the company.

Principal Service Commitments and System Requirements

Sablewick makes the following principal commitments to its customers in its customer agreement, its service level commitment and its public trust page:

- Security: customer traces and account data are protected through documented security measures, including encryption in transit and at rest, access granted by role and limited to those who require it, and a published channel for reporting security issues.
- Availability: the platform's trace ingestion and query services are committed to a monthly uptime target, with availability status published on a public status page.
- Customer data is not used to train any model, and hosted model providers engaged to score traces are contractually prohibited from training on it.
- Customers are notified of a security incident affecting their data without undue delay.

Sablewick establishes system requirements to meet these commitments, documented in its policy suite, its configuration standards and its risk register, including requirements for identity and access management, change management, monitoring and alerting, incident response, backup and recovery, vendor management, and the handling of data sent to hosted model providers.

Components of the System

Infrastructure

The production environment runs on Amazon Web Services (AWS) in a single directly administered cloud account and consists of containerized application services, a managed PostgreSQL database, object storage for trace data and backups, and the provider's logging, monitoring and audit trail services. Backups run daily and are retained in a second region. Development and staging environments are separate and hold synthetic data only.

Software

The platform comprises the Sablewick ingestion service, evaluation service and web application. Supporting software services include GitHub for source control and continuous integration, with a protected main branch and required automated checks; Google Workspace as the identity provider and for email and document collaboration; a password manager for workforce credentials; a monitoring platform for alerting and log aggregation; an issue tracker used for remediation and deficiency tracking; and a documentation workspace holding the policy suite, procedures and registers. Two hosted model providers are used to score customer traces.

People

The system is operated by the two founders described above. People engaged by the company, including contractors, are subject to background screening, a Code of Conduct, security awareness training, and security and confidentiality responsibilities stated in their role definition or contractor agreement. Offboarding follows a checklist generated from the SaaS asset inventory and records the removal timestamp for each system. Because the company is operated by two people, the functions that cannot be separated between them are identified and the compensating controls relied on instead, principally automated enforcement in the source control and deployment pipeline, are recorded and are tested in Section 4.

Procedures

Sablewick maintains documented policies and procedures supporting the system, including an information security policy suite, an access provisioning and deprovisioning procedure with quarterly access reviews attested by both founders, a change management process built on pull requests to a protected main branch with required review and automated checks, an incident response plan fitted to a two person organization and exercised through an annual tabletop, backup and recovery procedures with periodic restoration testing, vendor management procedures with a vendor register and a pre engagement security review, and a register of the hosted model providers that receive customer data. The controls that support these procedures are stated in Section 4.

Data

The system processes customer prompt and response traces, evaluation scores, customer account data, and system and security logs. Data at rest is encrypted, and data in transit is protected using TLS 1.2 or higher. Trace content sent to a hosted model provider for scoring carries opaque customer references rather than customer identifiers, and a customer may disable third party model evaluation for its account.

System Boundaries

The boundaries of the Sablewick Platform system encompass the production ingestion, evaluation and web application services and their database and object storage; the supporting cloud infrastructure, monitoring and audit trail services; the identity provider, source control and continuous integration tooling through which access and change are administered; the hosted model providers that receive customer trace content for scoring; and the policies, procedures and people that operate them. Billing is performed by a third party payment processor that receives no customer trace data and sits outside the service boundary.

Subservice Organization

Sablewick uses Amazon Web Services (AWS) as a subservice organization to provide the cloud infrastructure hosting the production environment. The description of the system presented in this report uses the carve-

out method: the description includes only the controls of Sablewick and excludes the controls of the subservice organization. Sablewick monitors the subservice organization by obtaining and reviewing its SOC 2 Type II report and by reviewing provider status through the vendor register.

The following types of complementary subservice organization controls are assumed in the design of Sablewick's controls:

CRITERIA	COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS
CC6.4	The subservice organization is responsible for restricting physical access to the data center facilities housing the production infrastructure to authorized personnel.
CC6.4	The subservice organization is responsible for monitoring the data center facilities housing the production infrastructure.
CC6.1	The subservice organization is responsible for the security of the virtualization and host operating system layers underlying the managed compute, database and storage services.
A1.2	The subservice organization is responsible for the redundancy and durability of the managed database and object storage services on which backups are retained.

Complementary User Entity Controls

Sablewick's controls were designed with the assumption that certain controls would be implemented by user entities. Each user entity's internal control must be evaluated in conjunction with Sablewick's controls and the related tests and results described in Section 4 of this report.

CRITERIA	COMPLEMENTARY USER ENTITY CONTROLS
CC6.2	User entities are responsible for managing the user accounts and credentials issued to their personnel, including maintaining the confidentiality of passwords and of the API keys issued to them for trace submission.
CC6.2, CC6.3	User entities are responsible for administering access for their own users, including removing access promptly when personnel no longer require it.
CC6.7	User entities are responsible for determining what content they submit to the service, including whether to exclude sensitive or regulated data from the traces they send, and for electing whether third party model evaluation is enabled for their account.
CC7.2	User entities are responsible for notifying the service organization promptly of suspected unauthorized access or misuse of the service.

Security Incidents

No security incidents were identified that (a) resulted from controls that were not suitably designed or did not operate effectively, or (b) otherwise required disclosure under the description criteria, during the period July 1, 2025 to June 30, 2026. A recorded retrieval of the incident register returned one entry for the period, an availability incident on November 3, 2025 in which the trace ingestion endpoint was unavailable for 71 minutes following a configuration change. No customer data was accessed, altered or disclosed, and the incident was resolved the same day.

Significant Changes to the System

No changes occurred during the period July 1, 2025 to June 30, 2026 that would be likely to affect report users' understanding of how the Sablewick Platform system was used to provide the service.

Report Use

The description does not omit or distort information relevant to the Sablewick Platform system, while acknowledging that 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 each individual report user may consider important to its own particular needs.

SECTION 4

Trust Services Criteria, Related Controls, and Tests of Controls

The tests described below were performed to evaluate whether the controls specified in management's description operated effectively throughout the period July 1, 2025 to June 30, 2026. Procedures consisted of inquiry of management and inspection of documents, system configurations and system generated records. Except where a procedure states otherwise, each population was tested in full: the complete population was obtained by a recorded retrieval that can be re-run, reconciled against an independent source where one exists, and every item in it was tested. Where a test rests on the state of a system configuration, coverage across the period was established from recorded configuration captures taken at the opening of the period, at each quarterly checkpoint and at the period end, together with the configuration change logs covering the intervals between them.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specific controls. Our tests of the control environment included (a) inspection of Sablewick's organizational structure, including segregation of functional responsibilities, and its policies and procedures; (b) inquiries of management and personnel responsible for developing, ensuring adherence to, and applying controls; and (c) inspection of documents and records pertaining to controls.

Where system-generated reports, queries, exports, and listings were used in the performance of our tests, we performed procedures to assess the completeness and accuracy of that information, including inspection of the recorded retrieval commands and unedited outputs from which each population was drawn, sequence and boundary testing of the populations, and reconciliation against independent records where an independent source exists.

Tests were performed over the complete population of occurrences for each control, except where the description of the test states that a sample was used; for each such control, the selection method and the reason full retrieval was impracticable are stated with the test.

Controls that operate through the configuration of an in-scope system were evaluated over the period through configuration captures taken at the start of the period, at quarterly checkpoints on October 1, 2025 and January 1, 2026 and April 1, 2026, and at the end of the period, together with each system's configuration change log covering the intervals between captures. Where the change log of a system does not cover an interval, that limitation is stated above.

This section is presented in three parts. Part 4.1 presents each applicable trust services criterion together with the controls Sablewick has designed to address it and the result of the service auditor's tests of each control. Part 4.2 presents each control with the criteria it addresses and the same result. Part 4.3 presents, for each control, the control as specified by Sablewick, the detailed tests of controls performed by Y Assurance PLLC, and the results of those tests. In the electronic version of this report, control references link to the detailed tests in Part 4.3 and criteria references link to Part 4.1. Management's responses to the exceptions identified in this section are presented in Section 5, which is not covered by the service auditor's report.

4.1 Trust Services Criteria and Related Controls

Each applicable trust services criterion is presented below with the controls that address it. Because a control may support more than one criterion, controls appear under each criterion to which they are mapped. The result shown for each control reflects the service auditor's tests of the control, presented in full in Part 4.3.

CC1 · CONTROL ENVIRONMENT	
CC1.1 The entity demonstrates a commitment to integrity and ethical values.	
GOV-01 · Code of Conduct & Ethics	No exceptions noted
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
GOV-02 · Governance Oversight	No exceptions noted
GOV-04 · Leadership & Advisor Oversight of Security	No exceptions noted
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
GOV-03 · Organizational Structure & Responsibilities	No exceptions noted
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
PPL-01 · Background Checks	No exceptions noted
PPL-02 · Job Descriptions & Competency	No exceptions noted
PPL-03 · Training & Competency Development	No exceptions noted
PPL-05 · Key Personnel & Continuity	No exceptions noted
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
GOV-01 · Code of Conduct & Ethics	No exceptions noted
PPL-04 · Performance & Accountability	No exceptions noted
PPL-06 · Contractor & Outsourced Personnel Controls	No exceptions noted
CC2 · COMMUNICATION AND INFORMATION	
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
AST-01 · Information Asset Inventory	No exceptions noted
AST-02 · Data Classification	No exceptions noted
AST-03 · SaaS & Data Asset Inventory	No exceptions noted
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
PPL-03 · Training & Competency Development	No exceptions noted
POL-02 · Policy Communication & Accessibility	No exceptions noted
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	
COM-01 · Customer Commitments & Service Descriptions	No exceptions noted
COM-02 · External Reporting & Inbound Communication	No exceptions noted
CC3 · RISK ASSESSMENT	
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
POL-01 · Policy Suite & Governance	No exceptions noted
RSK-01 · Annual Risk Assessment	No exceptions noted

CC3.2 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.	
RSK-01 · Annual Risk Assessment	No exceptions noted
CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
RSK-01 · Annual Risk Assessment	No exceptions noted
CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	
RSK-01 · Annual Risk Assessment	No exceptions noted
CC4 · MONITORING ACTIVITIES	
CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
EVL-01 · Ongoing Control Monitoring & Evaluation	No exceptions noted
CC4.2 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.	
EVL-02 · Deficiency Tracking & Remediation	No exceptions noted
CC5 · CONTROL ACTIVITIES	
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
RSK-02 · Risk-Based Control Design	No exceptions noted
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	
RSK-02 · Risk-Based Control Design	No exceptions noted
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
POL-01 · Policy Suite & Governance	No exceptions noted
CC6 · 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.	
AST-01 · Information Asset Inventory	No exceptions noted
AST-03 · SaaS & Data Asset Inventory	No exceptions noted
CHG-05 · Security Architecture Review	No exceptions noted
DAT-01 · Encryption at Rest & in Transit	No exceptions noted
DAT-04 · Production Data in Non-Production Environments	No exceptions noted
IAM-01 · User Authentication	No exceptions noted
IAM-02 · Multi-Factor Authentication	No exceptions noted
IAM-07 · Privileged Access Management	No exceptions noted
IAM-08 · Service Account & Infrastructure Credentials	No exceptions noted
IAM-11 · Third-Party App & OAuth Integration Review	No exceptions noted

NET-01 · Network Isolation	No exceptions 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. User system credentials are removed when user access is no longer authorized.	
IAM-03 · User Access Provisioning	No exceptions noted
IAM-04 · User Access Deprovisioning	**Exceptions noted**
IAM-09 · Access Review Founder Attestation	No exceptions 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.	
IAM-06 · Role-Based Access & Least Privilege	No exceptions noted
IAM-07 · Privileged Access Management	No exceptions noted
IAM-09 · Access Review Founder Attestation	No exceptions noted
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
Addressed by complementary subservice organization controls (see Section 3).	
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.	
DAT-02 · Secure Data & Asset Disposal	No occurrences
DAT-03 · Data Retention & Deletion	No exceptions noted
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
IAM-02 · Multi-Factor Authentication	No exceptions noted
IAM-11 · Third-Party App & OAuth Integration Review	No exceptions noted
NET-02 · Boundary Protection	No exceptions 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.	
AI-03 · Customer Data Boundaries for AI Features	No exceptions noted
AI-04 · AI Interaction Logging & Retention	No exceptions noted
AST-02 · Data Classification	No exceptions noted
DAT-01 · Encryption at Rest & in Transit	No exceptions noted
DAT-03 · Data Retention & Deletion	No exceptions noted
DAT-04 · Production Data in Non-Production Environments	No exceptions noted
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.	
END-02 · Software Installation Controls	No exceptions noted
END-03 · Endpoint Protection Founder-Managed Devices	No exceptions noted

CC7 · 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.	
VUL-01 · Vulnerability Scanning	No exceptions noted
VUL-04 · Dependency & Platform Update Management	No exceptions 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.	
AVL-02 · Availability Monitoring & Uptime Response	No exceptions noted
MON-01 · Security Logging	No exceptions noted
MON-02 · Security Alerting & Event Triage	No exceptions 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.	
MON-02 · Security Alerting & Event Triage	No exceptions 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.	
INC-02 · Incident Response Execution	No exceptions noted
INC-03 · Incident Response Solo Operator	No exceptions noted
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	
INC-02 · Incident Response Execution	No exceptions noted
INC-04 · Post-Incident Review & Corrective Actions	No occurrences
CC8 · 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.	
BCP-01 · BCP/DR Plan & Testing	No exceptions noted
CHG-02 · Emergency Change Process	No occurrences
CHG-03 · Environment Separation	No exceptions noted
CHG-04 · Secure Development Lifecycle	No exceptions noted
CHG-06 · Change Control Automated Gates	**Exceptions noted**
CC9 · RISK MITIGATION	
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
BCP-01 · BCP/DR Plan & Testing	No exceptions noted
BCP-02 · Data Backup & Recovery Infrastructure	No exceptions noted
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	
AI-01 · AI Provider Inventory & Data-Use Terms	No exceptions noted
AI-02 · Model Provider Data-Use Configuration	No exceptions noted
VND-01 · Vendor Risk Management	**Exceptions noted**

VND-02 · Subservice Organization Monitoring	No exceptions noted
VND-04 · Subprocessor Change Management & Notification	No exceptions noted
ADDITIONAL CRITERIA FOR AVAILABILITY	
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	
AVL-01 · Capacity Monitoring & Planning	No exceptions noted
AVL-02 · Availability Monitoring & Uptime Response	No exceptions noted
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	
BCP-02 · Data Backup & Recovery Infrastructure	No exceptions noted
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
BCP-01 · BCP/DR Plan & Testing	No exceptions noted
BCP-02 · Data Backup & Recovery Infrastructure	No exceptions noted

The production infrastructure is housed in facilities operated by the subservice organization; Sablewick operates fully remotely and maintains no facilities housing the system. Accordingly, criterion CC6.4 is addressed by the complementary subservice organization controls identified in Section 3. Certain criteria are also supported by the complementary user entity controls identified in Section 3.

4.2 Controls, Related Criteria, and Results

Each control is listed once below with the criteria it addresses and the result of the service auditor's tests of the control.

CONTROL	CRITERIA ADDRESSED	RESULT OF TESTS
AI & MODEL GOVERNANCE		
AI-01 · AI Provider Inventory & Data-Use Terms	CC9.2	No exceptions noted
AI-02 · Model Provider Data-Use Configuration	CC9.2	No exceptions noted
AI-03 · Customer Data Boundaries for AI Features	CC6.7	No exceptions noted
AI-04 · AI Interaction Logging & Retention	CC6.7	No exceptions noted
ASSET & DATA MANAGEMENT		
AST-01 · Information Asset Inventory	CC2.1, CC6.1	No exceptions noted
AST-02 · Data Classification	CC2.1, CC6.7	No exceptions noted
AST-03 · SaaS & Data Asset Inventory	CC2.1, CC6.1	No exceptions noted
AVAILABILITY		
AVL-01 · Capacity Monitoring & Planning	A1.1	No exceptions noted
AVL-02 · Availability Monitoring & Uptime Response	A1.1, CC7.2	No exceptions noted
BUSINESS CONTINUITY & DISASTER RECOVERY		
BCP-01 · BCP/DR Plan & Testing	CC9.1, A1.3, CC8.1	No exceptions noted

CONTROL	CRITERIA ADDRESSED	RESULT OF TESTS
BCP-02 · Data Backup & Recovery Infrastructure	CC9.1, A1.2, A1.3	No exceptions noted
CHANGE MANAGEMENT		
CHG-02 · Emergency Change Process	CC8.1	No occurrences
CHG-03 · Environment Separation	CC8.1	No exceptions noted
CHG-04 · Secure Development Lifecycle	CC8.1	No exceptions noted
CHG-05 · Security Architecture Review	CC6.1	No exceptions noted
CHG-06 · Change Control Automated Gates	CC8.1	**Exceptions noted**
CONTROL MONITORING		
EVL-01 · Ongoing Control Monitoring & Evaluation	CC4.1	No exceptions noted
EVL-02 · Deficiency Tracking & Remediation	CC4.2	No exceptions noted
DATA PROTECTION		
DAT-01 · Encryption at Rest & in Transit	CC6.1, CC6.7	No exceptions noted
DAT-02 · Secure Data & Asset Disposal	CC6.5	No occurrences
DAT-03 · Data Retention & Deletion	CC6.5, CC6.7	No exceptions noted
DAT-04 · Production Data in Non-Production Environments	CC6.7, CC6.1	No exceptions noted
ENDPOINT SECURITY		
END-02 · Software Installation Controls	CC6.8	No exceptions noted
END-03 · Endpoint Protection Founder-Managed Devices	CC6.8	No exceptions noted
EXTERNAL COMMUNICATION		
COM-01 · Customer Commitments & Service Descriptions	CC2.3	No exceptions noted
COM-02 · External Reporting & Inbound Communication	CC2.3	No exceptions noted
GOVERNANCE & ETHICS		
GOV-01 · Code of Conduct & Ethics	CC1.1, CC1.5	No exceptions noted
GOV-02 · Governance Oversight	CC1.2	No exceptions noted
GOV-03 · Organizational Structure & Responsibilities	CC1.3	No exceptions noted
GOV-04 · Leadership & Advisor Oversight of Security	CC1.2	No exceptions noted
IDENTITY & ACCESS MANAGEMENT		
IAM-01 · User Authentication	CC6.1	No exceptions noted
IAM-02 · Multi-Factor Authentication	CC6.1, CC6.6	No exceptions noted
IAM-03 · User Access Provisioning	CC6.2	No exceptions noted
IAM-04 · User Access Deprovisioning	CC6.2	**Exceptions noted**
IAM-06 · Role-Based Access & Least Privilege	CC6.3	No exceptions noted
IAM-07 · Privileged Access Management	CC6.3, CC6.1	No exceptions noted
IAM-08 · Service Account & Infrastructure Credentials	CC6.1	No exceptions noted
IAM-09 · Access Review Founder Attestation	CC6.2, CC6.3	No exceptions noted
IAM-11 · Third-Party App & OAuth Integration Review	CC6.1, CC6.6	No exceptions noted

CONTROL	CRITERIA ADDRESSED	RESULT OF TESTS
INCIDENT RESPONSE		
INC-02 · Incident Response Execution	CC7.4, CC7.5	No exceptions noted
INC-03 · Incident Response Solo Operator	CC7.4	No exceptions noted
INC-04 · Post-Incident Review & Corrective Actions	CC7.5	No occurrences
NETWORK & INFRASTRUCTURE		
NET-01 · Network Isolation	CC6.1	No exceptions noted
NET-02 · Boundary Protection	CC6.6	No exceptions noted
PEOPLE		
PPL-01 · Background Checks	CC1.4	No exceptions noted
PPL-02 · Job Descriptions & Competency	CC1.4	No exceptions noted
PPL-03 · Training & Competency Development	CC1.4, CC2.2	No exceptions noted
PPL-04 · Performance & Accountability	CC1.5	No exceptions noted
PPL-05 · Key Personnel & Continuity	CC1.4	No exceptions noted
PPL-06 · Contractor & Outsourced Personnel Controls	CC1.5	No exceptions noted
POLICY & DOCUMENTATION		
POL-01 · Policy Suite & Governance	CC5.3, CC3.1	No exceptions noted
POL-02 · Policy Communication & Accessibility	CC2.2	No exceptions noted
RISK MANAGEMENT		
RSK-01 · Annual Risk Assessment	CC3.1, CC3.2, CC3.3, CC3.4	No exceptions noted
RSK-02 · Risk-Based Control Design	CC5.1, CC5.2	No exceptions noted
SECURITY MONITORING		
MON-01 · Security Logging	CC7.2	No exceptions noted
MON-02 · Security Alerting & Event Triage	CC7.2, CC7.3	No exceptions noted
VENDOR MANAGEMENT		
VND-01 · Vendor Risk Management	CC9.2	**Exceptions noted**
VND-02 · Subservice Organization Monitoring	CC9.2	No exceptions noted
VND-04 · Subprocessor Change Management & Notification	CC9.2	No exceptions noted
VULNERABILITY MANAGEMENT		
VUL-01 · Vulnerability Scanning	CC7.1	No exceptions noted
VUL-04 · Dependency & Platform Update Management	CC7.1	No exceptions noted

4.3 Detailed Controls, Tests of Controls, and Results

For each control below, the control description presents the control as specified by Sablewick management, and the test procedures are those performed by Y Assurance PLLC to evaluate whether the control operated effectively throughout the period July 1, 2025 to June 30, 2026.

AI-01 · AI Provider Inventory & Data-Use Terms · Criteria: CC9.2

CONTROL DESCRIPTION

Sablewick maintains a register of the hosted model providers that process customer data, recording for each the provider, the models used, the categories of data sent, the contractual terms governing the provider's use of that data, and the date the terms were last reviewed. A provider is added to the register and its terms reviewed before customer data is sent to it.

AUDITOR'S TEST PROCEDURES

- Inspected the AI provider register to determine that each hosted model provider is recorded with the models used, the categories of customer data sent, and the contractual terms governing the provider's use of that data.
- Obtained the complete population of 2 hosted model providers in use during the period by a recorded retrieval from the AI provider register, reconciled against the application's outbound service configuration to determine that no provider receiving customer data was omitted, and inspected the executed terms for each to determine that the provider is contractually prohibited from training on customer data.

RESULTS

No exceptions noted.

AI-02 · Model Provider Data-Use Configuration · Criteria: CC9.2

CONTROL DESCRIPTION

Sablewick configures each hosted model provider account so that customer data sent to it is excluded from model training and is retained by the provider for no longer than the period stated in Sablewick's customer commitments. The configuration is recorded and reviewed when a provider is added or its terms change.

AUDITOR'S TEST PROCEDURES

- Inspected the account configuration of each of the 2 hosted model providers to determine that training on submitted data was disabled and that the provider side retention setting matched the period stated in the customer commitments, using the recorded configuration captures taken at the opening of the period, at each quarterly checkpoint and at the period end.
- Inspected the provider configuration review record to determine that the configuration was reviewed when a provider was added or its terms changed.

RESULTS

No exceptions noted.

AI-03 · Customer Data Boundaries for AI Features · Criteria: CC6.7

CONTROL DESCRIPTION

Sablewick defines and enforces the boundary of the customer data that may be sent to a hosted model provider. The application transmits only the trace content the customer has submitted for evaluation, customer identifiers are replaced with opaque references before transmission, and a customer may disable third party model evaluation for its account.

AUDITOR'S TEST PROCEDURES

- Inspected the data flow documentation and the application configuration governing outbound requests to hosted model providers to determine that the categories of data transmitted are limited to the trace content submitted for evaluation and that customer identifiers are replaced with opaque references before transmission.
- Inspected the account setting that disables third party model evaluation and its enforcement in the outbound request path to determine that a customer electing to disable evaluation has no customer data transmitted to a hosted model provider.

RESULTS

No exceptions noted.

AI-04 · AI Interaction Logging & Retention · Criteria: CC6.7

CONTROL DESCRIPTION

Sablewick logs the interactions its system has with hosted model providers, recording the provider, the model, the timestamp and the reference to the customer trace evaluated, and retains those logs for the period stated in its retention schedule. Prompt and response content is not written to the interaction log.

AUDITOR'S TEST PROCEDURES

- Inspected the interaction logging configuration and a recorded retrieval of log entries to determine that the provider, model, timestamp and trace reference are recorded and that prompt and response content is excluded from the log.
- Inspected the retention configuration applied to the interaction log store to determine that the retention period matched the retention schedule.

RESULTS

No exceptions noted.

AST-01 · Information Asset Inventory · Criteria: CC2.1, CC6.1

CONTROL DESCRIPTION

Sablewick maintains an inventory of its information assets, from infrastructure and applications to data stores and endpoints, each with a designated owner. The inventory and documented data flows are reviewed periodically for accuracy.

AUDITOR'S TEST PROCEDURES

- Inspected the data flow diagram to determine that the data flows between system components and external parties were documented.
- Inspected the asset inventory with owner column populated for each entry to determine that each asset had a designated owner.
- Inspected the asset inventory to determine that the inventory included all in-scope asset categories.
- Inspected the asset inventory spreadsheet and the related records to determine that the asset inventory existed and is maintained; and that the inventory was reviewed for accuracy at least annually.

RESULTS

No exceptions noted.

AST-02 · Data Classification · Criteria: CC2.1, CC6.7

CONTROL DESCRIPTION

Sablewick classifies data by sensitivity, with defined handling, storage, access, and disposal requirements per level, and communicates the scheme to personnel who handle data.

AUDITOR'S TEST PROCEDURES

- Inspected the training records to determine that the classification scheme was communicated to personnel who handle data.
- Inspected the asset inventory to determine that the key data assets were actually classified per the scheme.
- Inspected the data handling matrix to determine that each classification level had defined handling requirements (storage, access, transmission, disposal).
- Inspected the data classification policy to determine that the data classification scheme was defined.

RESULTS

No exceptions noted.

AST-03 · SaaS & Data Asset Inventory · Criteria: CC2.1, CC6.1

CONTROL DESCRIPTION

Sablewick maintains an inventory of the SaaS applications and tools it uses, identifying which hold customer or confidential data, reviews the inventory on a defined cadence, and adds new tools as they are adopted.

AUDITOR'S TEST PROCEDURES

- Inspected the SaaS and tool inventory to determine that each application in use was recorded with an owner, an update date, and an identification of whether it holds customer data.
- Obtained the complete population of 16 applications recorded in the inventory by a recorded retrieval, reconciled against the identity provider's connected application list and the corporate card transaction history to determine that no application in use was omitted from the inventory.
- Inspected the inventory review record to determine that the inventory was reviewed on the defined cadence and that applications adopted during the period were added.

RESULTS

No exceptions noted.

AVAILABILITY

AVL-01 · Capacity Monitoring & Planning · Criteria: A1.1

CONTROL DESCRIPTION

Sablewick monitors production system capacity, sets threshold-based alerts, evaluates capacity against current and forecasted demand, and initiates capacity changes when usage approaches defined tolerances.

AUDITOR'S TEST PROCEDURES

- Inspected the capacity review record to determine that the capacity was evaluated against current and forecasted demand at least annually.
- Inspected the auto-scaling configuration to determine that the capacity was scaled or expanded when usage approaches tolerances.
- Inspected the alert rule configuration to determine that the threshold-based alerts notified responsible personnel before capacity was exhausted.
- Inspected the monitoring platform to determine that the capacity metrics were monitored for production systems.

RESULTS

No exceptions noted.

AVL-02 · Availability Monitoring & Uptime Response · Criteria: A1.1, CC7.2

CONTROL DESCRIPTION

Sablewick monitors the uptime and health of production systems, alerts responsible personnel when availability degrades or an outage is detected, responds to and resolves availability incidents, and communicates system status to customers.

AUDITOR'S TEST PROCEDURES

- Inspected the monitoring platform's configured checks to determine that the health and uptime of the production services were monitored continuously throughout the period, using the recorded configuration captures taken at the opening of the period, at each quarterly checkpoint and at the period end.
- Inspected the alert routing configuration to determine that degradation or an outage notified the responder.
- Inspected the public status page to determine that availability status was communicated to customers.
- Obtained the complete population of 1 availability incident recorded during the period by a recorded retrieval from the monitoring platform, reconciled against the incident register, and inspected it to determine that it was responded to and resolved and that the resolution was recorded.

RESULTS

No exceptions noted.

BUSINESS CONTINUITY & DISASTER RECOVERY

BCP-01 · BCP/DR Plan & Testing · Criteria: CC9.1, A1.3, CC8.1

CONTROL DESCRIPTION

A documented BCP/DR plan identifies critical systems, recovery objectives, procedures, and responsible personnel. It is tested periodically, with results used to improve the plan and insurance considered for financial impact.

AUDITOR'S TEST PROCEDURES

- Inspected the recovery runbooks to determine that the recovery procedures were documented with responsible personnel.
- Inspected the BCP/DR plan section and the related records to determine that the critical systems were identified with recovery time and recovery point objectives; and that the plan was updated based on test findings.
- Inspected the BCP/DR plan document and the related records to determine that BCP/DR plan document existed; and that the system resilience requirements were considered in architecture decisions.
- Obtained the complete population of 2 recovery tests performed during the period by a recorded retrieval from the test records, and inspected each to determine that the plan tested within the last 12 months with results documented.

RESULTS

No exceptions noted.

BCP-02 · Data Backup & Recovery Infrastructure · Criteria: CC9.1, A1.2, A1.3

CONTROL DESCRIPTION

Automated backups run on schedule, monitored for success and stored in a geographically separate location, with restoration tested periodically. Environmental threats are mitigated and alternate processing infrastructure is available.

AUDITOR'S TEST PROCEDURES

- Inspected the backup configuration of the production database and object storage to determine that automated backups ran daily, that they were retained in a second region, and that the configuration held throughout the period, using the recorded configuration captures taken at the opening of the period, at each quarterly checkpoint and at the period end together with the configuration change log covering the intervals between them.
- Inspected the backup monitoring configuration and its alert history to determine that backup success and failure were monitored and that a failure notified the responder.
- Obtained the complete population of 2 restoration tests performed during the period by a recorded retrieval from the test records, and inspected each to determine that a backup was restored successfully and that the outcome, including the time taken, was recorded against the recovery objective.

RESULTS

No exceptions noted.

CHANGE MANAGEMENT

CHG-02 · Emergency Change Process · Criteria: CC8.1

CONTROL DESCRIPTION

Emergency changes follow a defined expedited process with retroactive documentation, approval, and post-implementation review. Incident-related changes are identified and tracked.

AUDITOR'S TEST PROCEDURES

- Inspected the emergency change procedure document to determine that the emergency change procedure existed.

RESULTS

No occurrences. The emergency change process was not invoked during the period. A recorded retrieval of the change records returned no change processed under the emergency procedure. Of the six changes deployed outside the standard release window, five followed the standard approval path; the sixth was deployed during the availability incident of November 3, 2025 using an administrative override rather than the emergency procedure, and is the exception reported at CHG-06. The design of the emergency change process was evaluated and is described above.

CHG-03 · Environment Separation · Criteria: CC8.1

CONTROL DESCRIPTION

Separate environments exist for development, staging, and production. Production data is not used in non-production environments without appropriate safeguards.

AUDITOR'S TEST PROCEDURES

- Inspected the access role comparison to determine that the access to production was restricted relative to non-production.
- Inspected the data masking configuration to determine that the production data was not used in non-production without safeguards.
- Inspected the cloud account structure to determine that the separate environments existed (development, staging, production).

RESULTS

No exceptions noted.

CHG-04 · Secure Development Lifecycle · Criteria: CC8.1

CONTROL DESCRIPTION

Sablewick incorporates security practices into the software development lifecycle. Secure coding standards, dependency management, and static or dynamic analysis are applied to reduce vulnerabilities introduced through development.

AUDITOR'S TEST PROCEDURES

- Inspected the secure development standard to determine that it covered security requirements, secure coding practices and security testing.
- Inspected the continuous integration pipeline configuration to determine that static analysis and secret scanning ran on every pull request and that a failing check blocked the merge.
- Inspected the dependency scanning configuration and its alert history to determine that dependencies were tracked and monitored for known vulnerabilities throughout the period.

RESULTS

No exceptions noted.

CHG-05 · Security Architecture Review · Criteria: CC6.1

CONTROL DESCRIPTION

New system architectures and significant design changes are reviewed for security implications before implementation.

AUDITOR'S TEST PROCEDURES

- Inspected the architecture review standard to determine that the criteria requiring a security review of a significant design change were defined.
- Obtained the complete population of 3 architecture changes recorded during the period by a recorded retrieval from the design records, reconciled against the change population to determine that no significant design change was omitted, and inspected the review record for each to determine that a security review was performed and recorded before deployment.

RESULTS

No exceptions noted.

CHG-06 · Change Control Automated Gates · Criteria: CC8.1

CONTROL DESCRIPTION

Changes to the production system are made through pull requests to a protected main branch. The branch protection configuration requires a review approval and the passing of automated test, dependency and secret scanning checks before a merge is permitted, and direct pushes to the protected branch are blocked. Deployment to production runs from the protected branch through an automated pipeline.

AUDITOR'S TEST PROCEDURES

- Inspected the branch protection configuration of the production repository to determine that a review approval and passing automated checks were required before merge and that direct pushes to the protected branch were blocked throughout the period, using the recorded configuration captures taken at the opening of the period, at each quarterly checkpoint and at the period end together with the repository configuration change log covering the intervals between them.
- Obtained the complete population of 812 changes deployed to production during the period by a recorded retrieval from the source control system, reconciled against the deployment pipeline history, and inspected each to determine that it was approved before it reached production and that the required automated checks passed.
- Inspected the deployment pipeline configuration and its run history to determine that production deployments originated from the protected branch.

RESULTS

Exceptions noted. For 1 of the 812 changes deployed to production during the period, the change reached production before the required review approval was recorded. The pull request was merged using an administrative override at 2:14 a.m. on November 3, 2025 during an active availability incident, and the approval was recorded 4 hours and 21 minutes after the change reached production. The required automated test, dependency and secret scanning checks ran and passed before the merge. The remaining 811 changes were approved before reaching production with the required checks passed.

EVL-01 · Ongoing Control Monitoring & Evaluation · Criteria: CC4.1

CONTROL DESCRIPTION

Sablewick monitors the effectiveness of its controls through ongoing activities and a periodic evaluation. Monitoring evidence is produced by system dashboards, alerting and the quarterly access and vendor reviews; management records a review of the security posture at least annually; and an independent evaluation of the environment is obtained annually through a third party penetration test.

AUDITOR'S TEST PROCEDURES

- Inspected the monitoring dashboards, alert history and the quarterly review records to determine that monitoring produced evidence of control operation throughout the period.
- Inspected the annual security posture review record to determine that management reviewed the security posture during the period and recorded the outcome.
- Inspected the third party penetration test report to determine that an independent evaluation of the environment was performed during the period.

RESULTS

No exceptions noted.

EVL-02 · Deficiency Tracking & Remediation · Criteria: CC4.2

CONTROL DESCRIPTION

Control deficiencies are identified, assessed for severity, communicated to responsible parties and leadership, and tracked through remediation to completion.

AUDITOR'S TEST PROCEDURES

- Inspected the corrective action plan template to determine that the corrective action plans included assigned owners and timelines.
- Inspected the escalation procedure to determine that the process existed to communicate deficiencies to responsible parties and leadership.
- Inspected the deficiency management procedure to determine that the process existed to identify and assess control deficiencies by severity.
- Inspected the deficiency tracker for the period to determine that the remediation was tracked to completion.

RESULTS

No exceptions noted.

DAT-01 · Encryption at Rest & in Transit · Criteria: CC6.1, CC6.7

CONTROL DESCRIPTION

Data is encrypted at rest with industry-standard encryption for databases and storage, and in transit over TLS 1.2 or higher, with cryptographic keys managed through their lifecycle.

AUDITOR'S TEST PROCEDURES

- Inspected the KMS configuration to determine that the cryptographic keys were stored securely (not in source code or plaintext).
- Inspected the encryption configuration to determine that the encryption algorithms and key lengths met current standards.
- Inspected the TLS configuration to determine that the data in transit was encrypted using TLS or equivalent for all in-scope connections.
- Inspected the database encryption settings and the related records to determine that the data at rest was encrypted on all in-scope systems; and that the key rotation was performed or scheduled.

RESULTS

No exceptions noted.

DAT-02 · Secure Data & Asset Disposal · Criteria: CC6.5

CONTROL DESCRIPTION

Data and software are securely wiped or destroyed from physical assets before disposal, return, or repurposing. For cloud resources, storage and data are destroyed per provider procedures.

AUDITOR'S TEST PROCEDURES

- Inspected the data disposal policy to determine that the data disposal procedure existed.

RESULTS

No occurrences. No physical asset was disposed of, returned or repurposed during the period. A recorded retrieval of the asset register returned no disposal event. Cloud storage destruction on customer deletion requests is tested at DAT-03. The design of the procedure was evaluated and is described above.

DAT-03 · Data Retention & Deletion · Criteria: CC6.5, CC6.7

CONTROL DESCRIPTION

Sablewick defines retention periods for customer data, system logs and backups that align with its contractual commitments, and deletes or anonymizes data when those periods expire or when a customer submits a valid deletion request. Storage of company or customer data on endpoint devices and removable media is prohibited by policy.

AUDITOR'S TEST PROCEDURES

- Inspected the data retention schedule to determine that a retention period was defined for each category of customer data, system log and backup, and that the periods aligned with the commitments stated in the customer agreement.
- Inspected the lifecycle configuration applied to the object storage and log stores and the database deletion routine to determine that data was deleted or anonymized when its retention period expired.
- Inspected the acceptable use policy to determine that storage of company or customer data on endpoint devices and removable media was prohibited.

RESULTS

No exceptions noted.

DAT-04 · Production Data in Non-Production Environments · Criteria: CC6.7, CC6.1

CONTROL DESCRIPTION

Sablewick prohibits the use of production or customer data in development and test environments. Non-production environments are populated with synthetic data generated for the purpose, and access to the production data stores is restricted to the production environment.

AUDITOR'S TEST PROCEDURES

- Inspected the data handling policy to determine that the use of production or customer data in development and test environments was prohibited.
- Inspected the seed data configuration for the development and staging environments to determine that they were populated with synthetic data rather than production data.
- Inspected the network and credential configuration of the non-production environments to determine that they held no route or credential to the production data stores, and inspected management's written representation covering the period to determine that no production or customer data was copied into a non-production environment.

RESULTS

No exceptions noted.

END-02 · Software Installation Controls · Criteria: CC6.8

CONTROL DESCRIPTION

Installation and modification of software on production systems is restricted to authorized personnel through access controls and the change management process.

AUDITOR'S TEST PROCEDURES

- Inspected the CI/CD pipeline configuration requiring approval to determine that the software deployments followed the change management process.
- Inspected the production admin user list with business justification to determine that the production admin access list was limited and documented.
- Inspected the production access list to determine that the software installation on production was restricted to authorized personnel.

RESULTS

No exceptions noted.

END-03 · Endpoint Protection Founder-Managed Devices · Criteria: CC6.8

CONTROL DESCRIPTION

Every device used to access production is recorded in a device inventory naming the device and the person assigned to it. Disk encryption, a screen lock with a short idle timeout, and automatic operating system and application updates are enabled on each device, and the settings are captured directly from each device rather than through a management platform.

AUDITOR'S TEST PROCEDURES

- Inspected the device inventory to determine that it named each device used to access production and the person assigned to it, and reconciled it against the identity provider's recorded sign in devices to determine that no device was omitted.
- Inspected the recorded settings output captured from each of the 4 devices in the inventory, taken at the opening of the period, at each quarterly checkpoint and at the period end, to determine that disk encryption was enabled, that a screen lock with a short idle timeout was enforced, and that automatic operating system and application updates were enabled on each.

RESULTS

No exceptions noted.

COM-01 · Customer Commitments & Service Descriptions · Criteria: CC2.3

CONTROL DESCRIPTION

Sablewick documents its security commitments to customers in contracts, SLAs, privacy policies, or trust pages. Customer responsibilities, system objectives, and how the service operates are communicated to external users.

AUDITOR'S TEST PROCEDURES

- Inspected the customer agreement, the service level commitment and the public trust page to determine that the security and availability commitments made to customers were documented and available to customers.
- Compared the commitments stated in those documents against the commitments described in Section 3 of this report to determine that they were consistent.
- Inspected the shared responsibility statement on the trust page to determine that the responsibilities borne by the customer were documented and available to customers.
- Inspected the changelog published on the trust page to determine that changes to the commitments during the period were communicated to customers.

RESULTS

No exceptions noted.

COM-02 · External Reporting & Inbound Communication · Criteria: CC2.3

CONTROL DESCRIPTION

Sablewick publishes a security contact address and a vulnerability disclosure policy on its public trust page, so that a person outside the company can report a security issue without identifying themselves to anyone inside it. Reports arriving on that channel are recorded and routed into the incident response process for evaluation.

AUDITOR'S TEST PROCEDURES

- Inspected the public trust page to determine that a security contact address and a vulnerability disclosure policy were published and reachable without authentication, and that a report could be submitted without the reporter identifying themselves.
- Inspected the incident response procedure to determine that a report arriving on the external channel was routed to the responder and evaluated, and inspected the record of the channel's inbox for the period to determine that reports received were recorded and evaluated.

RESULTS

No exceptions noted.

GOV-01 · Code of Conduct & Ethics · Criteria: CC1.1, CC1.5

CONTROL DESCRIPTION

Sablewick maintains a Code of Conduct that sets expected standards of behavior for everyone working on its behalf, including contractors. Each person acknowledges it on engagement and re-acknowledges it annually, and violations are addressed through documented procedures.

AUDITOR'S TEST PROCEDURES

- Inspected the onboarding checklist to determine that Code of Conduct communication process was documented.
- Inspected the employee handbook section on disciplinary procedures to determine that the disciplinary process for violations was documented.
- Inspected the Code of Conduct document with approval date to determine that Code of Conduct document existed and was current.
- Inspected the re-acknowledgment records from the most recent annual cycle for the period to determine that Code of Conduct was acknowledged and re-acknowledged within the defined period.

RESULTS

No exceptions noted.

GOV-02 · Governance Oversight · Criteria: CC1.2

CONTROL DESCRIPTION

Oversight of the security and internal control program rests with the two founders, together with an outside technical advisor and the lead seed investor. Sablewick issues a written security and compliance update each quarter to an outside technical advisor and its lead investor, neither of whom holds an operational role in the company, and records the decisions and follow up items arising from it.

AUDITOR'S TEST PROCEDURES

- Inspected the governance charter to determine that a governance body is identified with responsibility for oversight of security and internal controls, and that at least one member holds no day to day operational role.
- Inspected the advisor engagement letter and the investor's background to determine that at least one member of the governance body possesses relevant security, technology or compliance experience.
- Obtained the complete population of 4 governance updates issued during the period by a recorded retrieval from the governance records, and inspected each to determine that security, compliance or risk was on the agenda and that decisions and follow up items were recorded and tracked.

RESULTS

No exceptions noted.

GOV-03 · Organizational Structure & Responsibilities · Criteria: CC1.3

CONTROL DESCRIPTION

Sablewick defines its organizational structure, authorities and responsibilities. A current organizational record names each person engaged by the company, their role and the reporting lines between them; security, compliance and customer data protection responsibilities are assigned to a named individual; and because the company is operated by two people, the functions that cannot be separated between them are identified and the compensating controls relied on instead are recorded.

AUDITOR'S TEST PROCEDURES

- Inspected the organizational record in effect at the start of the period and its revision issued during the period to determine that each named the people engaged, their roles and the reporting lines between them, and that the two records covered the period without a gap.
- Inspected the responsibility assignment record to determine that security, compliance and customer data protection responsibilities were assigned to a named individual throughout the period, and that responsibility for the key external relationships was assigned.
- Inspected the separation of duties analysis to determine that the functions that cannot be separated at the company's size were identified, and that the compensating controls relied on instead were recorded and are the controls tested elsewhere in this section.

RESULTS

No exceptions noted.

GOV-04 · Leadership & Advisor Oversight of Security · Criteria: CC1.2

CONTROL DESCRIPTION

Sablewick reports security and compliance status to its outside technical advisor and its lead investor on a quarterly cadence, keeping people independent of day to day engineering informed of the security program. Each update states open risks, remediation progress and compliance milestones rather than a general assurance.

AUDITOR'S TEST PROCEDURES

- Inspected the advisor engagement letter and the distribution list of the recurring update to determine that a person independent of day to day engineering is identified as a recipient of security and compliance information.
- Obtained the complete population of 4 leadership and advisor updates issued during the period by a recorded retrieval from the update records, and inspected each to determine that security or compliance status was included and conveyed substantive status rather than a generic mention.

RESULTS

No exceptions noted.

IAM-01 · User Authentication · Criteria: CC6.1

CONTROL DESCRIPTION

Sablewick requires users to be uniquely identified and authenticated before accessing production systems and business applications. Authentication mechanisms are appropriate for the sensitivity of the systems accessed.

AUDITOR'S TEST PROCEDURES

- Inspected the list of accounts not managed through the identity provider to determine that the standalone or local accounts were minimized and documented.
- Inspected the authentication policy to determine that the authentication strength was tiered by system sensitivity.
- Inspected the login page to determine that the authentication was required before system access is granted.
- Inspected the user list export from identity provider to determine that all users were uniquely identified (no shared accounts for interactive use).

RESULTS

No exceptions noted.

IAM-02 · Multi-Factor Authentication · Criteria: CC6.1, CC6.6

CONTROL DESCRIPTION

Multi-factor authentication is enforced for access to production infrastructure, the cloud console, the source code repository and the business applications that hold company or customer data. Access to those systems is federated through the identity provider, and the identity provider requires a second factor at sign in.

AUDITOR'S TEST PROCEDURES

- Inspected the identity provider's authentication policy and its per application assignments to determine that multi factor authentication was required for every in scope system throughout the period, using the recorded configuration captures taken at the opening of the period, at each quarterly checkpoint and at the period end together with the identity provider's configuration change log covering the intervals between them.
- Inspected the enrolment status of each of the 4 people engaged during the period to determine that a second factor was enrolled and active for each.
- Inspected the cloud console and source code repository account settings to determine that access was federated through the identity provider and that local password only sign in was disabled.

RESULTS

No exceptions noted.

IAM-03 · User Access Provisioning · Criteria: CC6.2

CONTROL DESCRIPTION

Prior to granting access, Sablewick registers and authorizes the user and documents the access granted. This applies to all access provisioning including new hires, role changes, contractor onboarding, and temporary access grants.

AUDITOR'S TEST PROCEDURES

- Inspected the access provisioning procedure and the related records to determine that the documented provisioning process existed; and that the policy required authorization before access is granted.
- Obtained the complete population of 2 access provisioning events during the period by a recorded retrieval from the identity provider and the onboarding records, and inspected each to determine that the access request and approval were documented.
- Inspected each of the 2 access provisioning events during the period to determine that the approval was from an authorized approver (manager or system owner).
- Inspected each of the 2 access provisioning events during the period to determine that the access granted matched the authorized request.

RESULTS

No exceptions noted.

IAM-04 · User Access Deprovisioning · Criteria: CC6.2

CONTROL DESCRIPTION

Sablewick removes system access when an employee or contractor engagement ends. Access to in scope systems is removed within one business day of the engagement end date, and offboarding is tracked on a checklist that records each system and the removal timestamp. The checklist is generated from the SaaS asset inventory so that each system holding company or customer data appears on it.

AUDITOR'S TEST PROCEDURES

- Inspected the offboarding procedure and the checklist template to determine that removal of access to in scope systems is required within one business day of the engagement end date and that each system and removal timestamp is recorded.
- Obtained the complete population of 2 departures during the period by a recorded retrieval from the contractor engagement records, reconciled against identity provider account status to determine that no departure was omitted from the population, and inspected the offboarding record and the resulting system access state for each to determine that access to each in scope system was removed within one business day of the engagement end date.

RESULTS

Exceptions noted. For 1 of the 2 departures during the period, access to one of the five in scope systems the contractor held access to was removed 9 days after the engagement end date, against a documented standard of one business day. The engagement ended on November 14, 2025; access to the identity provider and the source code repository was removed the same day, and the account in the issue tracking system remained enabled until November 23, 2025. The system audit log recorded no activity on the account after the engagement end date. The offboarding checklist in use at the time did not enumerate the issue tracking system.

IAM-06 · Role-Based Access & Least Privilege · Criteria: CC6.3

CONTROL DESCRIPTION

Access is granted based on job function using defined roles. Users receive only the minimum access required for their duties.

AUDITOR'S TEST PROCEDURES

- Inspected the IdP group assignments to determine that the access was assigned through roles or groups (not individual grants).
- Inspected the role definitions in identity provider to determine that the access roles were defined and documented.
- Obtained the complete population of 27 user accounts across the in scope systems by a recorded retrieval from each system's user export, and inspected each to determine that the role assignments aligned with job functions.

RESULTS

No exceptions noted.

IAM-07 · Privileged Access Management · Criteria: CC6.3, CC6.1

CONTROL DESCRIPTION

Privileged access is limited to personnel with a documented business need. Privileged and service accounts are inventoried with named owners, and privileged activity is logged.

AUDITOR'S TEST PROCEDURES

- Inspected the cloud audit logs to determine that the privileged activities were logged.
- Inspected the privileged access justification records to determine that each privileged user was authorized and had a documented business need.
- Inspected the privileged user list per system to determine that the privileged users were inventoried across all in-scope systems.

RESULTS

No exceptions noted.

IAM-08 · Service Account & Infrastructure Credentials · Criteria: CC6.1

CONTROL DESCRIPTION

Service accounts, API keys, and infrastructure credentials are registered, authorized, and managed throughout their lifecycle.

AUDITOR'S TEST PROCEDURES

- Inspected the secrets manager rotation configuration to determine that the service account credentials were rotated or had a defined expiration.
- Inspected the service account registry to determine that the service accounts were documented with owner and purpose.
- Inspected the service account review records for the period to determine that the service account review was performed (separate from user access reviews).

RESULTS

No exceptions noted.

IAM-09 · Access Review Founder Attestation · Criteria: CC6.2, CC6.3

CONTROL DESCRIPTION

Sablewick reviews access to in scope systems each quarter. Because a single person administers the production environment, the review is performed jointly by both founders against a user export pulled from each in scope system, and the review record states the accounts reviewed, the determination reached for each and the date performed. Access identified as no longer required is removed and the removal is recorded.

AUDITOR'S TEST PROCEDURES

- Inspected the access review procedure to determine that a quarterly review is defined, that it is performed against a system generated user export, and that both founders attest to the outcome.
- Obtained the complete population of 4 quarterly access reviews during the period by a recorded retrieval from the review records, and inspected each to determine that it covered every in scope system, that a determination was recorded for each account, and that it was attested by both founders within the quarter.
- Inspected the removal records arising from the reviews to determine that access identified as no longer required was removed and that the removal was recorded.

RESULTS

No exceptions noted.

IAM-11 · Third-Party App & OAuth Integration Review · Criteria: CC6.1, CC6.6

CONTROL DESCRIPTION

Sablewick maintains an inventory of third-party applications and integrations granted access to core systems through OAuth or API tokens, reviews that access on a defined cadence, and removes integrations that are unused or hold more access than they need.

AUDITOR'S TEST PROCEDURES

- Inspected the per-integration scope to determine that the third-party integrations were granted only the access scopes they required to function.
- Inspected the system-generated list of connected apps and integrations per core system to determine that an inventory of third-party applications and integrations granted OAuth or API access to core systems was maintained.
- Inspected the review records with dates for the period to determine that the connected integrations were reviewed on a defined cadence and unused or over-scoped integrations were removed.

RESULTS

No exceptions noted.

INCIDENT RESPONSE

INC-02 · Incident Response Execution · Criteria: CC7.4, CC7.5

CONTROL DESCRIPTION

When a security incident occurs, Sablewick executes its response program: containing the incident, investigating root cause, resolving vulnerabilities, restoring operations, communicating to affected parties, and documenting the response.

AUDITOR'S TEST PROCEDURES

- Obtained the complete population of 1 incident recorded during the period by a recorded retrieval from the incident register, reconciled against the monitoring platform's alert history and the public status page to determine that no incident was omitted from the register.
- Inspected the incident record to determine that the incident was contained and mitigated, that the affected systems were restored to an operational state, and that the response was recorded with a timeline and the actions taken.
- Inspected the incident record and the related remediation entries to determine that the root cause was investigated and determined, that the weaknesses identified were remediated, and that the parties owed notification under the communication protocol were notified.

RESULTS

No exceptions noted.

INC-03 · Incident Response Solo Operator · Criteria: CC7.4

CONTROL DESCRIPTION

Sablewick maintains an incident response plan fitted to an organization operated by two people. The plan names the responder and the escalation path to the second founder and the outside advisor, states the severity thresholds that trigger customer notification, and records the external parties to be engaged where the incident exceeds the capacity of the two person team. The plan is exercised annually through a documented tabletop.

AUDITOR'S TEST PROCEDURES

- Inspected the incident response plan to determine that it names the responder and the escalation path, defines severity levels and their response times, states the threshold and method for customer notification, and identifies the external parties to be engaged where an incident exceeds the capacity of the team.
- Inspected the tabletop exercise record to determine that the plan was exercised during the period and that the outcome and follow up items were recorded.

RESULTS

No exceptions noted.

INC-04 · Post-Incident Review & Corrective Actions · Criteria: CC7.5

CONTROL DESCRIPTION

Sablewick conducts a written review after incidents that cross a defined threshold, capturing what happened, the impact, and the corrective actions, and tracks those corrective actions through to completion.

AUDITOR'S TEST PROCEDURES

RESULTS

No occurrences. No incident meeting the threshold for a formal post incident review occurred during the period. A recorded retrieval of the incident register returned one entry, an availability incident on November 3, 2025 that did not meet the review threshold and did not affect customer data. The design of the process was evaluated and is described above.

NET-01 · Network Isolation · Criteria: CC6.1

CONTROL DESCRIPTION

System components are isolated by risk and function, production is separated from non-production, and access between segments follows least privilege.

AUDITOR'S TEST PROCEDURES

- Inspected the security group rules to determine that the access between network segments followed least-privilege rules.
- Inspected the cloud network configuration to determine that the production was isolated from non-production environments.
- Inspected the network architecture diagram to determine that the network architecture was documented.

RESULTS

No exceptions noted.

NET-02 · Boundary Protection · Criteria: CC6.6

CONTROL DESCRIPTION

Boundary protections restrict inbound traffic to the ports, protocols and sources required by the service, and every externally reachable endpoint is inventoried. All access to the production environment is to internet facing services over encrypted connections and authenticated through the identity provider; Sablewick operates no corporate network and no remote access gateway.

AUDITOR'S TEST PROCEDURES

- Inspected the list of public-facing endpoints to determine that the external access points were inventoried.
- Inspected the security group inbound rules to determine that the only required ports and protocols were permitted inbound.
- Inspected the WAF configuration to determine that the boundary protection mechanisms were configured.

RESULTS

No exceptions noted.

PPL-01 · Background Checks · Criteria: CC1.4

CONTROL DESCRIPTION

Sablewick performs background checks on all new personnel including contractors prior to or upon their start date, including at minimum criminal history and employment verification.

AUDITOR'S TEST PROCEDURES

- Inspected the policy language specifying timing requirement for background checks to determine that the policy required checks prior to or upon start date.
- Inspected the HR policy and the related records to determine that the policy required background checks for all personnel including contractors prior to or upon start date; and that the policy defined minimum check scope.
- Obtained the complete population of 4 people engaged during the period by a recorded retrieval from the engagement records, and inspected each to determine that the background check was completed.
- Inspected each of the 4 people engaged during the period to determine that the check scope met policy requirements.

RESULTS

No exceptions noted.

PPL-02 · Job Descriptions & Competency · Criteria: CC1.4

CONTROL DESCRIPTION

Sablewick maintains job descriptions defining required competencies and qualifications for key roles. Competence is evaluated and shortcomings are addressed.

AUDITOR'S TEST PROCEDURES

- Inspected the performance review process documentation to determine that the process existed to evaluate competency and address shortcomings.
- Inspected the job descriptions with competency sections to determine that the competency requirements were defined for key roles.
- Inspected the job descriptions to determine that the job descriptions existed for key roles.

RESULTS

No exceptions noted.

PPL-03 · Training & Competency Development · Criteria: CC1.4, CC2.2

CONTROL DESCRIPTION

Sablewick requires all personnel to complete security awareness training periodically and upon onboarding for new personnel, covering relevant security topics. Personnel in security-relevant roles receive role-specific technical training.

AUDITOR'S TEST PROCEDURES

- Inspected the training policy to determine that the training policy defined timing for new personnel and ongoing completion requirements.
- Inspected the training platform curriculum and the related records to determine that the security awareness training curriculum existed covering relevant security topics; and that the role-specific technical training requirements were defined.
- Obtained the complete population of 4 people engaged during the period by a recorded retrieval from the training records, and inspected each to determine that the security awareness training was completed within the defined period.
- Inspected each of the 4 people engaged during the period to determine that the role-specific training or continuing education was evidenced.

RESULTS

No exceptions noted.

PPL-04 · Performance & Accountability · Criteria: CC1.5

CONTROL DESCRIPTION

Security and confidentiality responsibilities are stated in the role definition or contractor agreement of each person engaged by Sablewick, and performance against those responsibilities is reviewed and recorded at least annually for each person. Consequences for failing to meet them are defined in the Code of Conduct.

AUDITOR'S TEST PROCEDURES

- Inspected the role definitions and contractor agreements to determine that security and confidentiality responsibilities were stated for each role.
- Inspected the Code of Conduct to determine that the consequences of failing to comply with security policies and procedures were defined.
- Obtained the complete population of 4 people engaged during the period by a recorded retrieval from the role and engagement records, and inspected the review record for each to determine that performance against the stated security and confidentiality responsibilities was reviewed and recorded within the defined period.

RESULTS

No exceptions noted. No failure to meet a stated security or confidentiality responsibility occurred during the period; a recorded retrieval of the disciplinary records returned no entry, so no corrective action was required.

PPL-05 · Key Personnel & Continuity · Criteria: CC1.4

CONTROL DESCRIPTION

Sablewick identifies key personnel dependencies for critical functions. The company records that production engineering rests with a single person, maintains written runbooks for deployment, restoration and incident handling sufficient for another engineer to operate the system, and holds recovery credentials for the cloud account and the domain registrar in escrow accessible to the second founder.

AUDITOR'S TEST PROCEDURES

- Inspected the continuity record to determine that key personnel for critical functions are identified, including the single point of dependency for production engineering.
- Inspected the deployment, restoration and incident runbooks and the escrow arrangement for recovery credentials to determine that continuity measures are documented and accessible to a person other than the dependent individual.

RESULTS

No exceptions noted.

PPL-06 · Contractor & Outsourced Personnel Controls · Criteria: CC1.5

CONTROL DESCRIPTION

Sablewick holds contractors and outsourced personnel who can reach production systems or customer data to the same personnel and access controls as employees, from signed confidentiality agreements before access through standard offboarding and periodic access reviews.

AUDITOR'S TEST PROCEDURES

- Obtained the complete population of 2 contractor engagements during the period by a recorded retrieval from the contractor records, and inspected each to determine that a signed confidentiality and security agreement was in place before access was granted.
- Inspected each of the 2 contractor engagements during the period to determine that the access was provisioned through the standard onboarding process and revoked promptly when the engagement ended.
- Inquired of management and inspected the user access review records to determine that the contractor accounts with production or customer data access were included in the population covered by periodic user access reviews.

RESULTS

No exceptions noted.

POL-01 · Policy Suite & Governance · Criteria: CC5.3, CC3.1

CONTROL DESCRIPTION

Sablewick maintains a formally approved policy suite covering the required security domains, from access control through business continuity. Each policy has a named owner, is reviewed periodically, and is put into action through operational procedures.

AUDITOR'S TEST PROCEDURES

- Inspected the security objectives document to determine that the security and compliance objectives were defined and aligned with commitments.
- Inspected the procedure documents to determine that the operational procedures existed that put policies into action.
- Inspected the policy cover pages and the related records to determine that each policy had an assigned owner; and that the policy communication process was documented.
- Inspected the policy documents and the related records to determine that the policies existed for access control, change management, incident response, data protection, acceptable use, vendor management, risk management, and business continuity; and that the policies were reviewed and approved at least annually.

RESULTS

No exceptions noted.

POL-02 · Policy Communication & Accessibility · Criteria: CC2.2

CONTROL DESCRIPTION

Sablewick's security policies, objectives and responsibilities are held in a location every person engaged by the company can reach, and changes to them are communicated to the people they affect. The channels for reporting a security concern and the boundaries of the system are documented and available to authorized users.

AUDITOR'S TEST PROCEDURES

- Inspected the change notification emails to determine that the policy and system changes were communicated to affected personnel.
- Inspected the training materials to determine that the security awareness training included instruction on where to find relevant policies.
- Inspected the policy repository to determine that the policies were stored in an accessible location.
- Inspected the incident response policy to determine that the incident reporting channels were documented and accessible.

RESULTS

No exceptions noted.

RSK-01 · Annual Risk Assessment · Criteria: CC3.1, CC3.2, CC3.3, CC3.4

CONTROL DESCRIPTION

Sablewick performs a formal risk assessment periodically covering: identification of internal and external threats, evaluation of vulnerabilities, estimation of likelihood and impact, and risk response decisions. The assessment includes vendor risks, fraud risks, changes to the business environment, systems, technology, and threats.

AUDITOR'S TEST PROCEDURES

- Inspected the threat analysis section in risk assessment and the related records to determine that the internal and external threats were analyzed; the fraud risk was assessed, including unauthorized access and insider threats; and that the assessment was performed within the last 12 months.
- Inspected the risk register and the related records to determine that the risks were identified across the organization (not limited to IT); the risk response was documented for each identified risk (accept, avoid, reduce, or share); and that the risk assessment was updated when significant changes occurred.
- Inspected the security objectives section in risk assessment and the related records to determine that the security and operational objectives were defined as the basis for risk identification; the risk significance was estimated (likelihood and impact); and that the technology and vendor relationship changes were assessed for risk impact.
- Inspected the risk assessment document and the related records to determine that the formal risk assessment had been conducted within the last 12 months; the vendor and third-party risks were included in the assessment; and that the separation of critical functions was evaluated as a fraud prevention measure.

RESULTS

No exceptions noted.

RSK-02 · Risk-Based Control Design · Criteria: CC5.1, CC5.2

CONTROL DESCRIPTION

Control activities are selected and designed to address the risks identified in the risk assessment, with a documented mapping showing how each risk is covered, including the IT general controls the business depends on.

AUDITOR'S TEST PROCEDURES

- Inspected the control matrix to determine that Sablewick documented which business processes depend on technology controls.
- Inspected the IT general controls documentation to determine that the general IT controls were implemented across logical access, system operations, and change management.
- Inspected the risk-to-control mapping with no unaddressed high/critical risks to determine that each significant risk was addressed by at least one control.
- Inspected the risk-to-control mapping matrix to determine that the controls were selected and designed to address identified risks.

RESULTS

No exceptions noted.

SECURITY MONITORING

MON-01 · Security Logging · Criteria: CC7.2

CONTROL DESCRIPTION

Security event logs (authentication, access changes, configuration changes, admin actions, system errors) are collected from in-scope systems. Logs are retained for at least the defined retention period and protected from tampering.

AUDITOR'S TEST PROCEDURES

- Inspected the log storage access controls to determine that the logs were protected from tampering.
- Inspected the log retention configuration in SIEM to determine that the log retention period met at least Sablewick's defined retention period and no less than 90 days.
- Inspected the log source configuration to determine that the log types included required categories.
- Inspected the SIEM or log aggregation platform to determine that the security event logs were collected from in-scope systems (centralized or per-system).

RESULTS

No exceptions noted.

MON-02 · Security Alerting & Event Triage · Criteria: CC7.2, CC7.3

CONTROL DESCRIPTION

Alerts cover anomalous or suspicious activity and are triaged by designated personnel, with events classified by severity and potential incidents escalated into the incident response process.

AUDITOR'S TEST PROCEDURES

- Inspected the escalation criteria in incident response to determine that the escalation criteria were defined for routing events to incident response.
- Inspected the event classification scheme in incident response to determine that the events were classified by severity.
- Inspected the SIEM alert rules to determine that the alert rules existed for key threat scenarios.
- Inspected the alert review records for the period to determine that each alert was reviewed and triaged within the defined timeframe.

RESULTS

No exceptions noted.

VND-01 · Vendor Risk Management · Criteria: CC9.2

CONTROL DESCRIPTION

Sablewick maintains a register of the vendors that support or have access to the system, recording for each the service provided, whether it processes customer data, the security review performed and the date of the most recent review. A vendor that will process customer data is subject to a documented security review before processing begins, covering the vendor's security posture and a data processing agreement, and vendors that process customer data are reviewed at least annually thereafter.

AUDITOR'S TEST PROCEDURES

- Inspected the vendor management procedure to determine that a security review is required before a vendor processes customer data, that the review criteria are defined, and that vendors processing customer data are reviewed at least annually.
- Obtained the complete population of 16 vendors in the vendor register by a recorded retrieval, reconciled against the SaaS asset inventory and the corporate card transaction history to determine that no vendor was omitted from the register, and inspected each entry to determine that the service, the customer data determination and the most recent review date were recorded.
- Inspected the review record for each of the 7 vendors that processed customer data during the period to determine that a security review was completed before processing began and that a data processing agreement was executed.

RESULTS

Exceptions noted. For 1 of the 7 vendors that processed customer data during the period, the security review was completed after processing began. The vendor was engaged on March 9, 2026 and began processing customer data on March 11, 2026; the documented security review, including review of the vendor's SOC 2 report and execution of a data processing agreement, was completed on April 22, 2026, 42 days after processing began. The review identified no findings. The remaining 6 vendors that processed customer data were reviewed before processing began.

VND-02 · Subservice Organization Monitoring · Criteria: CC9.2

CONTROL DESCRIPTION

Vendors whose controls the product depends on are identified, their SOC 2 reports (or equivalent) obtained and reviewed periodically, and the controls they operate documented.

AUDITOR'S TEST PROCEDURES

- Inspected the SOC 2 report review notes and documented vendor-operated controls to determine that the reports were reviewed and vendor-operated controls were documented.
- Inspected the SOC 2 report cover pages to determine that the reports covered the examination period.
- Inspected the SOC 2 Type II reports on file for each dependent vendor to determine that a SOC 2 report or equivalent was obtained for each dependent vendor.
- Inspected the vendor dependency list identifying which vendors' controls the product relies on to determine that the vendors whose controls your product depends on were identified and listed.

RESULTS

No exceptions noted.

VND-04 · Subprocessor Change Management & Notification · Criteria: CC9.2

CONTROL DESCRIPTION

Sablewick maintains a current, published list of subprocessors, follows a review step before adding a new subprocessor that will handle customer data, and notifies customers of subprocessor changes in line with its commitments.

AUDITOR'S TEST PROCEDURES

- Inspected the published subprocessor list to determine that a current list of subprocessors was maintained and made available to customers.
- Obtained the complete population of 1 subprocessor change during the period by a recorded retrieval from the subprocessor register, and inspected it to determine that adding a new subprocessor followed a review step before it handles customer data.
- Inspected the subprocessor change during the period to determine that the customers were notified of subprocessor changes in line with Sablewick's commitments.

RESULTS

No exceptions noted.

VUL-01 · Vulnerability Scanning · Criteria: CC7.1

CONTROL DESCRIPTION

Vulnerability scans run on a regular schedule and after significant changes, with findings prioritized by severity and remediated within the defined timelines. Configuration compliance is monitored.

AUDITOR'S TEST PROCEDURES

- Inspected the scan records correlated with significant change dates to determine that the scans were performed after significant changes.
- Inspected the scan report to determine that the findings were categorized by severity.
- Inspected the scan target configuration and the related records to determine that all in-scope systems were included in scan scope; and that the latest vulnerability scan was performed within Sablewick's defined scanning frequency interval.
- Inspected the finding remediation records for the period to determine that the remediation was completed within the defined timelines.

RESULTS

No exceptions noted.

VUL-04 · Dependency & Platform Update Management · Criteria: CC7.1

CONTROL DESCRIPTION

Sablewick enables automated dependency update and security alerting for production repositories, defines a window for addressing vulnerable dependencies by severity, and remediates flagged advisories within that window.

AUDITOR'S TEST PROCEDURES

- Inspected the policy or standard to determine that Sablewick defined a window for remediating vulnerable dependencies by severity.
- Inspected the dependency tooling configuration to determine that the automated dependency update or security alerting was enabled for production repositories.
- Inspected the resolved dependency alerts for the period to determine that the vulnerability was addressed within Sablewick's defined window.

RESULTS

No exceptions noted.

SECTION 5

Other Information Provided by Sablewick That Is Not Covered by the Service Auditor's Report

Management's Response to Testing Exceptions

CHG-06 · Change Control Automated Gates

The administrative override that permitted the merge was removed from the repository configuration on November 4, 2025. Emergency changes now follow the documented emergency change process, which records the approval before the merge and requires a retrospective review within one business day. We reviewed the change in question and confirmed it introduced no security or availability regression.

VND-01 · Vendor Risk Management

The security review for this vendor was completed on April 22, 2026 and identified no findings that would have changed the decision to engage it. We have added a required checklist item to the vendor engagement process in our issue tracker so that the security review is recorded as complete before any production credential is issued to a vendor.

IAM-04 · User Access Deprovisioning

We removed the account on November 23, 2025 upon identifying it and confirmed from the system audit log that no activity occurred on the account after the engagement end date. The offboarding checklist was revised on November 24, 2025 to enumerate every in scope system, and it is now generated from the SaaS asset inventory so that a system added to the inventory appears on the checklist automatically. The second departure in the period was offboarded against the revised checklist with no exception.