Thoropass™
Assurance

patchworks

System and Organization Controls

(SOC) 2 Type 2 Report

Patchworks Media Ltd's Description of the Patchworks Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period August 1, 2025 to July 31, 2026

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report

SECTION 2

Assertion of Patchworks Media Ltd Management

SECTION 3

Description of the Patchworks Platform Throughout the Period August 1, 2025 to July 31, 2026

SECTION 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

SECTION 5

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

SECTION 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Patchworks Media Ltd ("Patchworks" or "the Company")

Scope

We have examined Patchworks' accompanying description of the Patchworks Platform found in Section 3 titled "Description of the Patchworks Platform Throughout the Period August 1, 2025 to July 31, 2026" (description), based on the criteria for a description of a service organization's system set forth 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), in AICPA, Description Criteria (description criteria)* and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Patchworks' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria*.

Patchworks uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Patchworks, to achieve Patchworks' service commitments and system requirements based on the applicable trust services criteria. The description presents Patchworks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Patchworks' 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 information included in Section 5, "Other Information Provided by Patchworks That Is Not Covered by the Service Auditor's Report", is presented by Patchworks' management to provide additional information and is not part of Patchworks' description of its Patchworks Platform made available to user entities throughout the period August 1, 2025 to July 31, 2026. Information included in Patchworks' 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

Patchworks 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 Patchworks' service commitments and system requirements were achieved. In Section 2, Patchworks has provided the accompanying assertion titled "Assertion of Patchworks Media Ltd Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Patchworks 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 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 operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 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 controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA, and we have complied with those requirements. In addition, we applied the Statements on Quality Control Standards established by the AICPA, and, accordingly, maintain a comprehensive system of quality control.

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 report users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any 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 the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories" of this report.

Opinion

In our opinion, in all material respects—

a. The description presents the Patchworks Platform that was designed and implemented throughout the period August 1, 2025 to July 31, 2026, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Patchworks' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in

the design of Patchworks' controls throughout that period.

c. The controls stated in the description operated effectively throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Patchworks' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Patchworks' 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 Patchworks, user entities of the Patchworks Platform during some or all of the period August 1, 2025 to July 31, 2026, business partners of Patchworks subject to risks arising from interactions with the Patchworks Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Thoropass Assurance

Arlington, Virginia
November 6, 2026

SECTION 2

Assertion of Patchworks Media Ltd Management

Assertion of Patchworks Media Ltd Management

We have prepared the accompanying description in Section 3 titled "Description of the Patchworks Platform Throughout the Period August 1, 2025 to July 31, 2026" (description), based on the criteria for a description of a service organization's system set forth 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), in AICPA, Description Criteria (description criteria)*. The description is intended to provide report users with information about the Patchworks Platform that may be useful when assessing the risks arising from interactions with Patchworks' system, particularly information about system controls that Patchworks has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria*.

Patchworks uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Patchworks, to achieve Patchworks' service commitments and system requirements based on the applicable trust services criteria. The description presents Patchworks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Patchworks' controls. The description does not disclose the actual controls at the subservice organization.

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

a. The description presents the Patchworks Platform that was designed and implemented throughout the period August 1, 2025 to July 31, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Patchworks' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of Patchworks' controls throughout that period.
c. The controls stated in the description operated effectively throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Patchworks' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Patchworks' controls operated effectively throughout that period.

Patchworks Media Ltd

SECTION 3

Description of the Patchworks Platform

Description of the Patchworks Platform Throughout the Period August 1, 2025 to July 31, 2026

Overview of Operations

Patchworks Media Ltd ("Patchworks" or "the Company") offers the Patchworks Platform, an Integration Platform as a Service (IPaaS) for retail and ecommerce businesses. The Patchworks Platform allows businesses to connect their core business applications to key ecommerce systems allowing retailers to simplify technology stack integration. The Patchworks Platform also eliminates the need for manual data entry by automating the flow of data across the business.

The system description in this section of the report details the Patchworks Platform. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance and security of the Patchworks Platform. The Terms of Service and Service Level Objectives include the communication of the Company's commitments to its customers.

System requirements are specifications that define the design and operation of the Patchworks Platform in order to meet the Company's principal commitments to customers. These requirements are specified in the Company's policies and procedures, system design documentation, contractual obligations, and applicable laws and regulations.

The Company's principal service commitments and system requirements related to the Patchworks Platform include the following:

Security Service Commitment and System Requirements

Patchworks will use commercially reasonable efforts to prevent any unauthorized use, access, processing, destruction, loss or disclosure of any customer data stored or processed by the Patchworks Platform.

To meet this commitment, the Company has established system requirements, including:

- Change Management
- Encryption Standards
- Identity and Access Management
- Network Security and Segmentation
- Policy Management and Governance
- Security Awareness Training
- Security Incident Response
- Security Monitoring and Reporting
- Threat and Vulnerability Management
- Vendor Risk Management

Availability Service Commitment and System Requirements

Patchworks will guarantee a 99.5% uptime for the Patchworks Platform exclusive of service outages attributed to (i) scheduled maintenance of which customers have notice; (ii) failures by customers, customer third party providers, suppliers or any factors beyond Patchworks' reasonable control; and (iii) internet connectivity issues (customers cannot connect to the internet).

To meet this commitment, the Company has established system requirements, including:

- Business Continuity and Disaster Recovery

- Capacity and Performance Management
- Data Backup, Recovery, and Replication
- System and Infrastructure Monitoring

Confidentiality Service Commitments and System Requirements

Patchworks will: (i) not use any customer confidential data except as necessary to exercise its rights or perform its obligations under the Terms of Service or as expressly authorized in writing; (ii) use the same degree of care to protect customer confidential data as it uses to protect its own confidential data of like nature; and (iii) not disclose customer confidential data to any person or entity except those with a need to know and who have entered into written confidentiality agreements.

To meet these commitments, the Company has established system requirements, including:

- Data Classification
- Data Retention and Secure Disposal
- Encryption of Confidential Data
- Information Sharing and Confidentiality Standards

The Components of the System Used to Provide the Service

The boundaries of the Patchworks Platform include the aspects of the Company's infrastructure, software, people, procedures, and data that are necessary to deliver the service and directly support its operation. Supporting functions that are integral to the operation and control of the service (for example, IT support and human resources) are also considered within the system boundaries. Functions and activities that do not directly or indirectly contribute to the delivery, security, or availability of the service are excluded from the boundaries of the Patchworks Platform.

The subsections below describe the components that support the operation of the Patchworks Platform.

Infrastructure

The Company utilizes Amazon Web Services (AWS) as a subservice organization to provide infrastructure and data hosting services that support the Patchworks Platform. By leveraging the resiliency, scalability, and security features of these infrastructure services, the Company is able to host and operate the Patchworks Platform in a secure and reliable manner that meets current and future demand.

The Company remains responsible for designing, configuring, and maintaining the system architecture within AWS to ensure that security, availability, and resiliency requirements are met.

The in-scope hosted infrastructure components are outlined in the table below:

Infrastructure Component	Business Function	Hosted Location
Amazon Aurora MySQL	Data Storage	AWS
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	AWS
Amazon Elastic Kubernetes Service (EKS)	Container Orchestration	AWS
Amazon Simple Storage Service (S3)	Data Storage	AWS
AWS Key Management Service (KMS)	Cryptographic Key Management	AWS

Infrastructure Component	Business Function	Hosted Location
AWS Security Groups	Network Traffic Control	AWS

Software

The Company leverages software components to operate the Patchworks Platform and deliver services to its customers. These include applications, platforms, and supporting tools used to build, secure, monitor, and maintain the environment. The Company remains responsible for selecting, implementing, and maintaining these software components to ensure that applicable system requirements are met.

The in-scope software components are outlined in the table below:

Software Component	Business Function
AWS Backup	Backup and Restore
AWS Config	Configuration Management
Composer Audit	Code and Dependency Scanning
GitHub	Code Repository
GitHub Actions	Continuous Integration and Delivery
Google Workspace	Single Sign-On (SSO) and Authentication
Grafana	Infrastructure Monitoring
HubSpot	Ticketing System
Jira	Ticketing System
Prometheus	Infrastructure Monitoring
Slack	Alert Communication
Terraform	Configuration Management
Wazuh	Threat Detection

People

The Company's personnel are responsible for operating, securing, and supporting the Patchworks Platform. Personnel perform activities necessary to deliver the Company's services, including governance, operations, customer support, and security-related functions. The Company remains responsible for recruiting, training, and

overseeing personnel to ensure that their roles are performed in accordance with applicable policies and requirements.

The in-scope personnel roles and responsibilities are outlined in the table below:

Role/Unit Name	Responsibilities
Customer Success	Responsible for managing and strengthening customer relationships to drive adoption, satisfaction, and retention of products and services.
Engineering	Responsible for the design, development, testing, deployment, and maintenance of software and system components.
Executive Management	Responsible for providing strategic leadership, overseeing company-wide activities, and ensuring organizational goals and objectives are established, communicated, and achieved.
Human Resources	Responsible for managing the employee lifecycle, including recruitment, onboarding, role definition, performance management, and terminations, while ensuring compliance with employment laws and policies.
Marketing	Responsible for developing and executing marketing strategies to enhance brand awareness and generate leads.
Product	Responsible for defining product vision, strategy, and roadmap, gathering customer requirements, and coordinating with stakeholders to deliver features that meet market and business needs.
Sales	Responsible for revenue generation, client acquisition, and management of the sales pipeline.

Procedures

The Company relies on documented automated and manual procedures to govern the operation, security, and support of the Patchworks Platform. These procedures are maintained in alignment with the Company's Information Security Policy and are reviewed and updated as necessary for changes in the business, but no less than annually. The Company remains responsible for developing, implementing, and maintaining these procedures to ensure they are followed consistently and support the Company's operational and compliance objectives.

The in-scope procedures are outlined in the table below:

Procedure	Description
Access Control	How the Company restricts access to its systems, provisions and removes access rights, and prevents unauthorized access.
Asset Management	How the Company tracks and manages its assets, including hardware and software, to ensure accurate records, compliance with requirements, and protection of resources.

Procedure	Description
Business Continuity and Disaster Recovery	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Change Management	How the Company identifies, reviews, and implements system changes using a controlled process to prevent unauthorized or untested changes.
Data Backup and Recovery	How the Company manages and tests data backups to ensure restorations can occur if needed.
Data Classification, Handling, and Retention	How the Company classifies data, establishes requirements for its secure handling and storage, determines retention periods in compliance with requirements, and securely disposes of records when no longer needed.
Incident Management	How the Company detects, reports, responds to, and manages incidents that could affect the operation or protection of the system, in order to minimize impact and support recovery.
Monitoring and Logging	How the Company collects, reviews, and analyzes system activity logs and alerts to detect and respond to unusual or unauthorized activity.
Risk and Vendor Management	How the Company identifies, assesses, and mitigates risks to the system, including risks arising from business disruptions, operations, and the use of vendors and business partners by evaluating, selecting, and monitoring vendors to ensure they meet security and compliance requirements.
Security Awareness and Training	How the Company trains personnel on security and compliance requirements and monitors completion of training activities.
System Operations	How the Company manages and monitors system operations and responds to deviations, including security-related events.

Data

Data refers to transaction streams, files, data stores, tables, and other outputs used or processed by the Patchworks Platform. While the Company maintains data necessary for the operation and support of the Patchworks Platform, customers remain responsible for defining and controlling the data they provide and maintain within the Patchworks Platform. The Company remains responsible for managing and protecting that data in accordance with its policies, contractual commitments, and applicable regulatory requirements.

Encryption is enabled for data stores housing customer data. Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.

System Incidents

A system event is defined as an occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in Patchworks' failure to achieve its service commitments or system requirements. Such an

occurrence may arise from actual or attempted access or use by internal or external parties and may:

- Impair or potentially impair the availability, integrity, or confidentiality of information or systems.
- Result in unauthorized disclosure or theft of information or other assets, or the destruction or corruption of data.
- Cause damage to systems.

Such occurrences also may arise from the failure of the Patchworks Platform to process data as designed or from the loss, corruption, or destruction of data used by the Patchworks Platform.

On the other hand, a system incident is defined as a system event that requires action on the part of Patchworks management to prevent or reduce the impact of the event on Patchworks' achievement of its service commitments and system requirements.

There were no identified significant system incidents that (a) resulted from controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements, or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements throughout the period August 1, 2025 to July 31, 2026.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- **Availability:** Information and systems are available for operation and use to meet the entity's objectives.
- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all the trust services categories; for example, the criteria related to risk assessment apply to the Security, Availability, and Confidentiality categories. As a result, the trust services criteria for the Security, Availability, and Confidentiality categories are organized into (a) the criteria that are common to all the trust services categories (common criteria) and (b) additional specific criteria applicable only to a single category. The common criteria are suitable for evaluating the effectiveness of controls to achieve the entity's system objectives related to the security category; no additional control activity criteria are needed. For the categories of Availability and Confidentiality, a complete set of criteria consists of (a) the common criteria and (b) the control activity criteria applicable to each specific trust services category being reported on. The criteria for each trust services category being reported on are considered complete only if all the criteria associated with that category are addressed.

The common criteria are organized as follows:

1. **Control Environment:** The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. **Information and Communication:** The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. **Risk Assessment:** The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. **Monitoring Activities:** The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.

5. **Control Activities:** The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. **Logical and Physical Access Controls:** The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. **System Operations:** The criteria relevant to how the entity manages the operation of a system and detects and mitigates processing deviations, including logical and physical security deviations.
8. **Change Management:** The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. **Risk Mitigation:** The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the Security, Availability, and Confidentiality categories.

Control Environment

Integrity and Ethical Values

Patchworks places emphasis on ethics and communication within the organization. Management communicates and oversees the Code of Conduct, which defines expected responsibilities and behavior regarding data and information system usage. All personnel are required, upon hire, to acknowledge in writing that they have received, read, and understood its contents.

Patchworks demonstrates its commitment to integrity in all interactions with customers, vendors, and personnel by maintaining documented policies that establish ethical and business conduct standards. These policies guide decision-making, reinforce accountability, and support the control environment.

As part of its compliance framework, Patchworks maintains an inventory of third-party service providers that support the system. These providers are contractually obligated to adhere to information security requirements and to report cybersecurity incidents in a timely manner, ensuring that vendor practices align with Patchworks' integrity and security requirements.

Oversight and Authority

The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function. The Risk Committee meets quarterly and maintains formal meeting minutes.

Organizational Structure

Patchworks' organizational structure provides a framework for planning, executing, and controlling business operations. Roles and responsibilities are formally documented, communicated, and assigned to ensure adequate staffing, operational efficiency, segregation of duties, and oversight of the security and control environment. Management has also established clear authority levels and reporting lines for key personnel to maintain accountability. Patchworks follows a formal onboarding program to assist new personnel as they become familiar with organizational processes, systems, policies, and procedures. This structure supports alignment of responsibilities with the Company's internal control, compliance, and security objectives.

Management's Philosophy and Operating Style

Patchworks' management adopts an active and engaged approach to business operations, maintaining close communication with the workforce and key vendor representatives. Management emphasizes ethical conduct, responsibility, and compliance with established policies across all areas of the organization.

The leadership team is directly involved in setting strategic objectives, overseeing operational activities, and reinforcing the importance of security, confidentiality, and integrity in daily practices. This operating style promotes a culture of transparency, responsiveness, and proactive risk management, ensuring that decisions align with the

Company's objectives and requirements.

Authority and Responsibility

Patchworks assigns appropriate levels of authority and responsibility to personnel across the organization to facilitate effective internal control. Roles and responsibilities are documented and communicated through job descriptions, policies, and procedures to ensure individuals understand their obligations in maintaining security and compliance.

Oversight mechanisms are in place to review and approve critical activities, ensuring that responsibilities are appropriately segregated to reduce the risk of conflicts of interest and unauthorized actions.

Human Resources

All new personnel are subject to pre-employment screening, such as reference or background checks, consistent with the Company's hiring practices, before being granted access to production systems or sensitive data. As part of the onboarding process, personnel are also required to review and sign confidentiality agreements, reinforcing their obligation to safeguard company and customer information and prohibiting unauthorized disclosure of data.

The Company follows a structured onboarding program to familiarize new personnel with security policies, operational processes, and role-specific responsibilities. Information security training is mandatory upon hire and reinforced through annual refresher training to ensure personnel understand the Company's security practices, their role in protecting systems and data, and key concepts such as cybersecurity threats, phishing and social engineering, malware, secure data handling, authentication practices, and incident reporting. Supplemental awareness campaigns and targeted communications are also used to strengthen security awareness throughout the year.

The Company has implemented a performance management process to provide feedback, assess effectiveness, and align individual objectives with organizational goals.

Information and Communication

Patchworks maintains an Information Security Policy that defines the information security rules and requirements for the service environment. The policy is reviewed and approved by management and communicated to all relevant personnel.

Processes are in place to ensure that critical information related to security, system availability, and compliance objectives is communicated effectively both internally and externally. Management ensures that personnel receive timely updates on new or revised policies, control requirements, and operational procedures through established communication channels such as internal knowledge bases, scheduled briefings, and formal announcements.

The Company maintains documented guidance describing how personnel should escalate incidents, compliance concerns, or process deviations. Communication lines are structured to ensure that information reaches the appropriate decision-makers without unnecessary delay, including mechanisms for reporting control exceptions and protocols for sharing updates with clients and vendors.

To promote transparency with stakeholders, Patchworks provides documentation describing service features, security practices, and compliance measures. This documentation is reviewed and updated periodically to reflect changes in systems or requirements.

Risk Assessment and Mitigation

Patchworks maintains a formal risk assessment process to identify, evaluate, and manage risks that could affect its objectives and the delivery of secure, reliable services. Each identified risk is evaluated and rated to ensure that appropriate controls are designed and implemented to mitigate the most significant threats to the Company's systems and operations.

The risk assessment is conducted annually and updated in response to significant changes in technology, operations, regulatory requirements, business strategy, or other emerging risks. This ensures new risks are

identified and addressed in a timely manner.

Patchworks applies a structured methodology that includes:

- Identifying threats – considering internal and external factors such as technology, operations, personnel, vendor dependencies, and regulatory changes.
- Analyzing vulnerabilities – assessing weaknesses in processes, technology, and personnel that could expose the Company to exploitation.
- Estimating likelihood of impact – evaluating the probability that a vulnerability could be successfully exploited.
- Assessing severity of impact – analyzing potential consequences, including operational, financial, reputational, and regulatory implications.
- Ranking and prioritizing risks – combining likelihood and impact ratings to establish a risk score and guide remediation priorities.

Assessment results are reviewed by management and used to inform the design and implementation of controls, security policies, and ongoing risk mitigation activities. Mitigation strategies include implementing preventive and detective controls, monitoring key risk indicators, and formally tracking remediation activities through completion.

The process is integrated into the Company's governance, risk, and compliance (GRC) framework to ensure that risks are continuously identified, evaluated, and addressed in strategic planning and operational decision-making.

Vendor Management

Patchworks maintains a Vendor Management Policy that governs the selection, onboarding, and ongoing oversight of third-party service providers. The policy includes requirements for classifying vendors based on criticality, assessing risks associated with the procurement of third-party services, and reviewing vendor performance on an ongoing basis.

Formal agreements are established with all critical vendors, and these agreements include commitments applicable to the services provided. To ensure that vendor controls remain effective, Patchworks obtains and reviews third-party attestation reports or performs a vendor risk assessment on an annual basis. Exceptions or control gaps identified in these reviews are evaluated to determine their potential impact on the Patchworks Platform and addressed through remediation or compensating measures where necessary.

Through these activities, vendor risks are identified, monitored, and mitigated as part of Patchworks' broader GRC framework.

Monitoring

The systems within the boundary are configured to support continuous monitoring, detection, alerting, and testing for vulnerabilities and threats. Management reviews system alerts promptly and supports monitoring through preventive, detective, and corrective audit logging. Relevant monitoring outputs are shared with executive and management personnel to ensure timely awareness and action.

Vulnerability Management and Testing

Patchworks maintains a documented Vulnerability Management Policy that defines methods for identifying vulnerabilities, assessing their severity, and prioritizing remediation or mitigation activities within defined timelines. The policy provides the framework for consistent execution of vulnerability management practices.

In alignment with this policy, Patchworks performs both automated and manual security testing at regular intervals. Code dependency vulnerability scans are performed on a scan-on-push basis to identify, quantify, and prioritize vulnerabilities. Infrastructure supporting the service is patched as a part of routine maintenance to help ensure that systems supporting the service are hardened against security threats. Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment. Identified vulnerabilities are ranked and remediated in accordance with the Company's Vulnerability Management Policy and related procedures.

Threat Monitoring and Logging

The Company employs log management tools to monitor and analyze security events and trends that may impact its ability to achieve security objectives. A system monitoring tool is utilized to monitor system availability and performance and generates alerts when specific, predefined thresholds are met. An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches and generates alerts when security events occur. Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and enabled on production infrastructure.

Alerting and Escalation

The Company employs a distributed monitoring approach that combines commercially available tools, custom code, and instant messaging platforms. This system attributes critical security events to their source and sends targeted alerts to authorized personnel with the authority and context necessary to validate them. Alerts are reviewed by authorized personnel, who address them when appropriate or escalate to designated teams for resolution.

Control Activities

Patchworks has implemented documented policies, procedures, and technical controls to mitigate identified risks and support the Company's objectives and requirements. Control activities are designed and implemented across the organization, embedded into business processes, and aligned with objectives for safeguarding systems and data. These activities include:

- **Governance and Policy Controls** – Documented policies and standards that define responsibilities and expected practices for personnel.
- **Technical and Monitoring Controls** – Safeguards and monitoring mechanisms designed to prevent, detect, and respond to unauthorized or anomalous activity.
- **Operational Controls** – Processes that integrate security and compliance practices into daily operations.
- **Third-Party Oversight Controls** – Oversight of vendors and service providers through contractual requirements, risk assessments, and periodic reviews.

Together, these control activities form a structured framework that mitigates risks to the service and supports the Company's objectives and requirements.

Logical Access

Patchworks maintains a documented Access Control Policy that defines the requirements for provisioning and deprovisioning users, performing access reviews and recertifications, and restricting access based on separation of duties and least privilege. Access reviews are conducted to confirm that system access remains appropriate and access is modified or removed as necessary. Password configurations for system components are enforced in accordance with Patchworks' Password Policy.

Access to system components is based on job role and function, and requires a documented request with manager approval prior to provisioning. Users are assigned unique user IDs before being granted access. Access rights are assigned using Role-Based Access Control (RBAC) and the principle of least privilege, ensuring users are granted only the access required for their job duties. Privileged access to system components is restricted to authorized users with a business need, and access to production infrastructure requires valid multi-factor authentication (MFA) tokens. Access to system components is revoked within 24 hours of termination as part of the termination process.

System Operations

Patchworks maintains a documented Incident Response Policy that establishes a structured process for preparing for, detecting, responding to, and recovering from incidents. The policy also defines requirements for analysis, communication, follow-up, and training to strengthen resilience and improve future response. Personnel responsibilities during a breach, the steps for managing an incident, and the importance of information security

awareness are documented and communicated to all personnel.

The Incident Response Team employs industry-standard procedures such as identification, verification, classification, and prioritization to drive effective resolution during business-impacting events. Alerts are reviewed, triaged, and escalated according to severity, ensuring timely involvement of technical and management stakeholders.

Post-mortems are convened after any significant operational issue, regardless of whether external impact occurred. Findings are documented to capture the root cause, identify lessons learned, and track preventative or corrective actions to completion. The incident response plan is tested annually to assess the effectiveness of the incident response program.

Change Management

Patchworks maintains a documented Change Management Policy to guide the processes for requesting, documenting, reviewing, approving, testing, scheduling, and implementing changes. All changes are recorded in a centralized system of record to ensure traceability, accountability, and auditability. Changes that may affect system availability, security, or confidentiality are communicated to management and any affected partners.

System configuration standards are documented and implemented to ensure systems and network devices are securely configured. Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.

Secure Software Development: Patchworks applies a systematic approach to software development so that changes to customer-impacting services are reviewed, tested, approved, and communicated. Prior to deployment, changes are:

- Developed in an environment segregated from production.
- Reviewed by authorized personnel for accuracy, appropriateness, and security impact.
- Tested to confirm expected functionality and ensure performance and security are not adversely affected.
- Approved by authorized personnel to provide oversight and confirm that business impacts are understood.

Availability

System capacity is evaluated continuously to help ensure that processing capacity can meet demand. The risks that could prevent Patchworks from meeting its availability commitments and requirements include operational failures, performance issues, and service disruptions from natural or man-made disasters. The Company has designed its controls to address the following types of availability risks:

- Insufficient processing capacity.
- Insufficient internet response time.
- Loss of processing capability due to a power outage.
- Loss of communication with user entities due to a break in telecommunication services.
- Loss of key processing equipment, facilities, or personnel due to a natural disaster.

Availability risks are mitigated through capacity management, monitoring tools, backup and recovery processes, and documented business continuity and disaster recovery (BC/DR) plans. Daily backups are configured for databases housing customer data. Data backup restoration tests are performed annually to verify data recoverability. The BC/DR plan is tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.

In evaluating the suitability of its availability controls, Patchworks considers the commitments and requirements related to availability, the timeliness and reliability of backup and recovery procedures, and the ability to maintain continuity of critical services during operational disruptions.

Confidentiality

The confidentiality category refers to the protection of customer information as committed by the Company's service level agreements. Patchworks has designed and implemented confidentiality controls to mitigate risks of

improper use or disclosure of sensitive information, whether from internal or external sources.

Confidentiality risks are addressed through documented policies and procedures governing the classification, use, retention, and secure disposal of data. These policies are supported by confidentiality agreements, information-sharing restrictions, remote access controls, transmission safeguards, encryption of sensitive information, and vendor risk management processes.

Patchworks supports the effectiveness of these confidentiality measures by monitoring compliance with confidentiality obligations, considering potential causes of improper disclosure, and updating controls in alignment with regulatory requirements and industry best practices.

Complementary User Entity Controls (CUECs)

CUECs are controls that a user entity must implement, in combination with the Company's controls, for the Company's service commitments and system requirements to be achieved. In designing its controls, Patchworks management did not identify any CUECs that would be necessary, in combination with controls at Patchworks, to provide reasonable assurance that its principal service commitments and system requirements would be achieved. Accordingly, no CUECs are required to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

User entity responsibilities are activities that user entities must perform to obtain the intended benefit of the service. These responsibilities do not affect the Company's ability to achieve its service commitments and system requirements, but support each user entity's own control environment and effective use of the service. However, user entities remain responsible for implementing and maintaining their own internal controls to ensure the proper use of the Patchworks Platform within their environments. These responsibilities are intended to support each user entity's broader control environment, ensure the effective use of the services provided, and help user entities derive benefit from those services. The following responsibilities are illustrative and should not be considered a comprehensive listing.

User entities should:

- Report any material changes to their control environment that may impact the services performed by the Company, in accordance with contractually defined time frames.
- Notify the Company of any changes to vendor security requirements applicable to the services.
- Grant access only to authorized personnel with a legitimate business need, and promptly revoke or adjust access upon termination, role change, or when access is no longer required.
- Configure and periodically review user permission levels within the service to enforce the principle of least privilege.
- Restrict use of the service to authorized business purposes.
- Maintain physical security and environmental controls at their facilities and for remote workers.
- Implement controls for managing user credentials (e.g., IDs, passwords, and multi-factor authentication) and for securing endpoints used to access the Company's services.
- Maintain the confidentiality of authentication credentials assigned to their personnel and refrain from sharing accounts among multiple users.
- Notify the Company of any known or suspected security incidents.
- Ensure that any data used in connection with the service is appropriate for such use and complies with applicable laws and regulatory requirements.
- Maintain their own business continuity and disaster recovery plans to address disruptions to their use of the service.
- Maintain adequate connectivity and infrastructure necessary to access the service.
- Notify the Company of any planned changes to usage volume or patterns that could materially affect capacity or performance expectations.
- Classify and handle data shared with the Company in accordance with the data's confidentiality requirements, and communicate any special handling requirements to the Company per contractual terms.
- Restrict internal distribution of confidential reports, outputs, or data received from the Company to personnel

with a legitimate business need.
- Dispose of or return confidential information no longer needed in accordance with contractual and regulatory requirements.

Each user entity should assess its own control environment to determine whether additional responsibilities are needed to ensure the effective use of the services and to derive benefit from them.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization. The Company's controls related to the Patchworks Platform cover only a portion of the overall internal control for each user entity of the Patchworks Platform. The description does not extend to the services provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Accordingly, CSOCs are expected to be in place at AWS as described in the CSOC table below.

Through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Patchworks Platform to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	AWS is responsible for encrypting customer data at rest and in transit within the managed infrastructure to mitigate the risk of unauthorized access to customer data. AWS is responsible for implementing access control over the managed infrastructure to mitigate the risk of unauthorized access or privilege escalation.
CC6.4	AWS is responsible for restricting physical access to its data centers through approval and revocation processes, surveillance and access control mechanisms, periodic reviews of access rights, and retention of monitoring records to mitigate the risk of unauthorized access, intrusion, or physical tampering.
CC6.5	AWS is responsible for securely decommissioning production assets in its control and ensuring that data is rendered unreadable or unrecoverable through logical deletion, cryptographic erasure, or physical destruction once no longer required, to mitigate the risk of unauthorized recovery of data from retired equipment.
CC6.6	AWS is responsible for applying security patches to the managed infrastructure as part of routine maintenance to mitigate the risk of vulnerabilities being exploited due to outdated systems.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC7.2 A1.2	AWS is responsible for implementing and maintaining environmental protection measures at its data centers, including fire detection and suppression systems, temperature and humidity controls, uninterruptible power supply (UPS) units, backup power sources, and monitoring of environmental conditions, to mitigate the risk of outages, equipment failure, or data loss due to environmental hazards or power disruptions.
CC8.1	AWS is responsible for implementing managed infrastructure changes to mitigate the risk of unauthorized or untested changes affecting system availability, integrity, or confidentiality.
A1.2	AWS is responsible for replicating customer data within the managed infrastructure across multiple availability zones to mitigate the risk of data loss or service disruption resulting from the failure of a single facility or availability zone.

Specific Criteria Not Relevant to the System

There were no specific Security, Availability, and Confidentiality Trust Services Criteria as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria* that were not relevant to the system as presented in this report.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the Patchworks Platform was used to provide the service from August 1, 2025 to July 31, 2026.

Report Use

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

SECTION 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

This SOC 2 Type 2 Report was prepared in accordance with the AICPA Attestation Standards based on the criteria for a description of a service organization's system set forth 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), in AICPA, Description Criteria (description criteria)* and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 1, 2025 to July 31, 2026.

Description of Testing Procedures Performed

Thoropass Assurance evaluated the design and operating effectiveness of the controls listed in this section throughout the period August 1, 2025 to July 31, 2026. Our evaluation included procedures we considered necessary in the circumstances to determine whether the control activities were suitably designed and operating to achieve the service commitments and system requirements based on the relevant trust services criteria throughout the period August 1, 2025 to July 31, 2026.

In determining the nature, timing, and extent of procedures performed, we considered the following factors:

- The nature and timing of the controls being tested.
- The types of evidential matter.
- The appropriateness of the control design and operation relative to the applicable trust services criteria.
- The assessed level of control risk.
- The entity's control environment and related governance processes.

The procedures performed included:

- **Inquiry:** Conducted detailed interviews with relevant stakeholders to obtain evidence that the control operated during the period. This procedure was accompanied by additional testing, as noted below, to corroborate the information obtained through inquiry.
- **Observation:** Observed the performance of the control during the period to obtain evidence of the application of the specific control activity.
- **Inspection:** Inspected relevant documentation, configurations, and reports to obtain evidence that the control activity was designed and operating as intended.
- **Reperformance:** Obtained the documentation used in the performance of the control activity and independently reperformed the control or process to verify its accuracy and operation.

Reliability of Information Produced by Patchworks

For tests of controls requiring the use of information produced by the entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), a combination of the following procedures were performed, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

- Inspected the source of the IPE.
- Inspected the query, script, or parameters used to generate the IPE.
- Tied data between the IPE and the source.
- Inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity.

Furthermore, in addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access privileges); an inspection of management's procedures, as applicable, to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports was performed. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information was sufficiently precise and detailed for purposes of fully testing the controls identified by Patchworks.

This section of the report includes 2 tables:

Table 1: Patchworks Controls Mapped to the Security, Availability, and Confidentiality Criteria

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

Table 1: Patchworks Controls Mapped to the Security, Availability, and Confidentiality Criteria

Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.1	REQ-7 REQ-8 REQ-9 REQ-10 REQ-11 REQ-14	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	REQ-3 REQ-4	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.3	REQ-2 REQ-3 REQ-4 REQ-15 REQ-16	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	REQ-11 REQ-12 REQ-13 REQ-14 REQ-15	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	REQ-7 REQ-8 REQ-14 REQ-15	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Information and Communication		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC2.1	REQ-4 REQ-19 REQ-20 REQ-33 REQ-39 REQ-46 REQ-47 REQ-65	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	REQ-2 REQ-12 REQ-13 REQ-15 REQ-56	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	REQ-5 REQ-6 REQ-22	The entity communicates with external parties regarding matters affecting the functioning of internal control.

Risk Assessment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC3.1	REQ-17 REQ-18	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	REQ-17 REQ-19 REQ-23	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.
CC3.3	REQ-17 REQ-19	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	REQ-17 REQ-19 REQ-44 REQ-45 REQ-52	The entity identifies and assesses changes that could significantly impact the system of internal control.

Monitoring Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC4.1	REQ-4 REQ-19 REQ-20 REQ-23 REQ-44 REQ-45 REQ-46 REQ-47	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	REQ-4 REQ-19 REQ-20 REQ-23	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.

Control Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC5.1	REQ-17 REQ-20	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC5.2	REQ-17 REQ-20	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	REQ-1 REQ-17 REQ-21 REQ-24 REQ-32 REQ-42 REQ-48 REQ-51 REQ-53 REQ-60 REQ-65	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Logical and Physical Access Controls		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC6.1	REQ-24 REQ-25 REQ-26 REQ-27 REQ-33 REQ-34 REQ-35 REQ-36	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.
CC6.2	REQ-29 REQ-30 REQ-31	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	REQ-28 REQ-29 REQ-30 REQ-31 REQ-54 REQ-57	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.

Logical and Physical Access Controls		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC6.4	The Company's production environment is hosted at third-party data centers, which have been carved out for the purposes of this report.	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.
CC6.5	REQ-32 REQ-33	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.
CC6.6	REQ-27 REQ-35 REQ-37 REQ-40 REQ-43	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	REQ-35 REQ-39	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.
CC6.8	REQ-38 REQ-39 REQ-40 REQ-43	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

System Operations		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC7.1	REQ-19 REQ-42 REQ-46 REQ-47 REQ-51 REQ-52	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.
CC7.2	REQ-39 REQ-40 REQ-41 REQ-43 REQ-44 REQ-45 REQ-46 REQ-47	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.

System Operations		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC7.3	REQ-39 REQ-44 REQ-45 REQ-46 REQ-47 REQ-48	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.
CC7.4	REQ-43 REQ-48 REQ-49 REQ-50	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	REQ-48 REQ-49 REQ-50 REQ-58 REQ-59	The entity identifies, develops, and implements activities to recover from identified security incidents.

Change Management		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC8.1	REQ-43 REQ-51 REQ-53 REQ-54 REQ-55 REQ-57	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC9.1	REQ-17 REQ-48 REQ-49 REQ-58 REQ-59	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	REQ-21 REQ-22 REQ-23	The entity assesses and manages risks associated with vendors and business partners.

Additional Criteria for Availability

Availability		
Criteria	**Applicable Control Activities**	**Criteria Description**
A1.1	REQ-41 REQ-64	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	REQ-58 REQ-59 REQ-60 REQ-62	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.
A1.3	REQ-58 REQ-59 REQ-60 REQ-61	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Additional Criteria for Confidentiality

Confidentiality		
Criteria	**Applicable Control Activities**	**Criteria Description**
C1.1	REQ-22 REQ-32 REQ-65 REQ-66	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	REQ-32 REQ-67	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

Control activities and test procedures performed in connection with determining the design and operating effectiveness of controls relative to the applicable Trust Services Criteria are described below.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-1	An Information Security Policy is documented and defines the information security rules and requirements for the service environment. The policy is version controlled, reviewed annually, approved by management, and communicated to authorized users.	Inspected the Information Security Policy and policy repository to determine that an Information Security Policy was documented, defined the information security rules and requirements for the service environment, was version controlled, reviewed annually, approved by management, and communicated to authorized users.	No exceptions noted.
REQ-2	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the Information Security Policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
REQ-3	The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function.	Inspected the Risk Committee charter to determine that the Risk Committee was tasked with governance, oversight, and responsibilities relative to internal control and the Risk Committee included members that were independent of the internal control function.	No exceptions noted.
REQ-4	The Risk Committee meets quarterly and maintains formal meeting minutes.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine that the Risk Committee met quarterly and maintained formal meeting minutes.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-5	The Terms of Service and Service Level Objectives include the communication of the Company's commitments to its customers.	Inspected the Terms of Service and Service Level Objectives to determine that the Company's commitments were communicated to customers.	No exceptions noted.
REQ-6	Technical support resources related to system operations are provided on the Company's website.	Inspected the Company's website to determine that technical support resources related to system operations were provided on the Company's website.	No exceptions noted.
REQ-7	The Code of Conduct describes employee and contractor responsibilities and expected behavior regarding data and information system usage.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
REQ-8	Upon hire, employees and contractors acknowledge that they have read and agree to the Code of Conduct.	Inspected the Code of Conduct acknowledgments for a sample of new employees and contractors to determine that new employees and contractors received and acknowledged that they had read and agreed to the Code of Conduct upon hire.	No exceptions noted.
REQ-9	The employee and contractor confidentiality agreement prohibits any disclosure of information and other data to which the employee or contractor has been granted access.	Inspected the employee and contractor confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee or contractor had been granted access.	No exceptions noted.
REQ-10	Upon hire, employees and contractors acknowledge that they have read and agree to the confidentiality agreement.	Inspected the confidentiality agreement acknowledgments for a sample of new employees and contractors to determine that new employees and contractors received and acknowledged that they had read and agreed to the confidentiality agreement upon hire.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-11	New employees offered employment are subject to background checks prior to their start date.	Inspected the background check results for a sample of new employees to determine that new employees were subject to background checks prior to their start date.	No exceptions noted.
REQ-12	New employees and contractors complete security awareness training upon hire.	Inspected the training records for a sample of new employees and contractors to determine that new employees and contractors completed security awareness training upon hire.	No exceptions noted.
REQ-13	Employees and contractors complete security awareness training annually.	Inspected the training records for a sample of employees and contractors to determine that employees and contractors completed security awareness training annually.	No exceptions noted.
REQ-14	Managers complete performance appraisals for direct reports annually.	Inspected the performance appraisals for a sample of employees and contractors to determine that managers completed performance appraisals for direct reports annually.	No exceptions noted.
REQ-15	Job descriptions are documented for employees and contractors supporting the service and include authorities and responsibilities in support of the system.	Inspected the job descriptions for a sample of employees and contractors supporting the service to determine that job descriptions were documented and included authorities and responsibilities in support of the system.	No exceptions noted.
REQ-16	An organization chart is documented and defines the organizational structure and reporting lines.	Inspected the organization chart to determine that an organization chart was documented and defined the organizational structure and reporting lines.	No exceptions noted.
REQ-17	A Risk Management Policy is documented and includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that a Risk Management Policy was documented and included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-18	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	Inspected the risk assessment results to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	No exceptions noted.
REQ-19	A risk assessment is performed annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment results to determine that a risk assessment was performed annually and, as part of this process, threats and changes to service commitments were identified, risks were formally assessed, and the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	No exceptions noted.
REQ-20	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.	Inspected the risk assessment results to determine that as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks.	No exceptions noted.
REQ-21	A Vendor Management Policy is documented and includes guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	Inspected the Vendor Management Policy to determine that a Vendor Management Policy was documented and included guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-22	Formal agreements are in place with critical vendors. These agreements include commitments applicable to that entity.	Inspected the contracts for a sample of critical vendors to determine that formal agreements were in place with critical vendors and the agreements included commitments applicable to that entity.	No exceptions noted.
REQ-23	A third-party attestation report is reviewed annually for all critical vendors. Exceptions noted in the reports are evaluated to determine their impact on the service.	Inspected the third-party attestation report review results for a sample of critical vendors to determine that a third-party attestation report was reviewed annually for all critical vendors and exceptions noted in the reports were evaluated to determine their impact on the service.	No exceptions noted.
REQ-24	An Access Control Policy is documented and includes guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege	Inspected the Access Control Policy to determine that an Access Control Policy was documented and included guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege	No exceptions noted.
REQ-25	Authentication to the following system components requires unique usernames and passwords: - Network - Patchworks Platform - Operating System (OS) - Data Stores - AWS Console - Code Repository	Inspected the system configurations and observed login attempts to determine that authentication to the following system components required unique usernames and passwords: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-26	Passwords for the following system components are configured according to the Password Policy: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository	Inspected the Password Policy and compared to password configurations for the following system components to determine that passwords were configured according to the Password Policy: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository	No exceptions noted.
REQ-27	Access to production infrastructure is restricted to authorized users with valid multi-factor authentication (MFA) tokens.	Inspected the MFA configurations to determine that access to production infrastructure was restricted to authorized users with valid MFA tokens.	No exceptions noted.
REQ-28	Privileged access to the following system components is restricted to authorized users with a business need: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository	Inspected the system access listings, inquired of management, and compared each user's access privileges to their job role to determine that privileged access to the following system components was restricted to authorized users with a business need: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-29	Semi-annual access reviews are conducted to help ensure that system access is restricted appropriately for the following system components: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository The reviews are documented, and access is modified or removed where applicable.	Inspected the access review results for a sample of semi-annual periods to determine that semi-annual access reviews were conducted to help ensure that system access was restricted appropriately, the reviews were documented, and access was modified or removed where applicable for the following system components: - Network - Patchworks Platform - OS - Data Stores - AWS Console - Code Repository	Exceptions noted. For 1 of 1 sampled semi-annual periods, an access review was not completed.
REQ-30	Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.	Inspected the access request tickets for a sample of users that received access to system components to determine that access to system components was based on job role, function, and required a documented access request with manager approval prior to access being provisioned.	No exceptions noted.
REQ-31	Access to system components is revoked within 24 hours of termination as part of the termination process.	Inspected the termination tickets for a sample of terminated users to determine that access to system components was revoked within 24 hours of termination as part of the termination process. Inspected the listing of terminated users and compared against the privileged access system listings to determine that terminated users did not retain access to the system components after their separation.	No exceptions noted. No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-32	A Data Retention and Disposal Policy is documented and includes guidance for the secure retention and disposal of customer data.	Inspected the Data Retention and Disposal Policy to determine that a Data Retention and Disposal Policy was documented and included guidance for the secure retention and disposal of customer data.	No exceptions noted.
REQ-33	An inventory of production system assets is maintained by management.	Inspected the production system asset inventory to determine that an inventory of production system assets was maintained by management.	No exceptions noted.
REQ-34	Encryption is enabled for data stores housing customer data.	Inspected the encryption configurations to determine that encryption was enabled for data stores housing customer data.	No exceptions noted.
REQ-35	Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.	Inspected the transmission protocol configurations to determine that secure data transmission protocols were used to encrypt customer data when transmitted over public networks.	No exceptions noted.
REQ-36	The network is segmented to prevent unauthorized access to customer data.	Inspected the network configurations to determine that the network was segmented to prevent unauthorized access to customer data.	No exceptions noted.
REQ-37	AWS security groups are configured to prevent unauthorized access to the production environment.	Inspected the AWS security group configurations to determine that AWS security groups were configured to prevent unauthorized access to the production environment.	No exceptions noted.
REQ-38	Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and enabled on production infrastructure.	Inspected the anti-malware software configurations to determine that anti-malware technology was deployed for environments commonly susceptible to malicious attacks and was configured to be updated routinely, logged, and enabled on production infrastructure.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-39	A log management tool is utilized to monitor and identify security events and trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when security events occur.	Inspected the log management tool dashboard, configurations, and an example alert notification to determine that a log management tool was utilized to monitor and identify security events and trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when security events occurred.	No exceptions noted.
REQ-40	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches and generates alerts when security events occur.	Inspected the IDS dashboard, configurations, and an example alert notification to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection of potential security breaches and generated alerts when security events occurred.	No exceptions noted.
REQ-41	A system monitoring tool is utilized to monitor system availability and performance and generates alerts when specific, predefined thresholds are met.	Inspected the system monitoring tool dashboard, configurations, and an example alert notification to determine that a system monitoring tool was utilized to monitor system availability and performance and generated alerts when specific, predefined thresholds were met.	No exceptions noted.
REQ-42	A Vulnerability Management Policy is documented and includes guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines	Inspected the Vulnerability Management Policy to determine that a Vulnerability Management Policy was documented and included guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-43	Infrastructure supporting the service is patched as a part of routine maintenance to help ensure that systems supporting the service are hardened against security threats.	Inspected the infrastructure configurations to determine that infrastructure supporting the service was patched as a part of routine maintenance to help ensure that systems supporting the service were hardened against security threats.	No exceptions noted.
REQ-44	Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment.	Inspected the penetration test results to determine that penetration testing was performed annually to identify vulnerabilities that could have been exploited to gain access to the production environment.	Exceptions noted. An annual penetration test was not conducted during the audit period.
REQ-45	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	Inspected the remediation tickets for the critical and high vulnerabilities identified during the penetration test to determine that a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.	Exceptions noted. An annual penetration test was not conducted during the audit period.
REQ-46	Code dependency vulnerability scans are performed on a scan-on-push to identify, quantify, and prioritize vulnerabilities.	Inspected the vulnerability scan configurations and scan results to determine that code dependency vulnerability scans were performed on a scan-on-push basis to identify, quantify, and prioritize vulnerabilities.	No exceptions noted.
REQ-47	The vulnerability scanning tool is configured to block code from being deployed to production when vulnerabilities are identified during code dependency scans until identified vulnerabilities are remediated.	Inspected the vulnerability scanning tool configurations and an example blocked deployment to determine that the vulnerability scanning tool was configured to block code from being deployed to production when vulnerabilities were identified during code dependency scans until identified vulnerabilities were remediated.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-48	An Incident Response Policy is documented and includes guidance for detecting, responding to, and recovering from security events and incidents.	Inspected the Incident Response Policy to determine that an Incident Response Policy was documented and included guidance for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
REQ-49	The incident response plan is tested annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested annually to assess the effectiveness of the incident response program.	No exceptions noted.
REQ-50	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.	Inquired of management and inspected the security incident repository to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No security incidents occurred during the period.
REQ-51	Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.	Inspected the hardening standards to determine that hardening standards were documented and included guidance on baseline security requirements for production systems before deployment to the production environment.	No exceptions noted.
REQ-52	A configuration management tool (CMT) is used to ensure that system configurations are deployed consistently throughout the environment.	Inspected the CMT configurations to determine that a CMT was used to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
REQ-53	A Change Management Policy is documented and includes guidance for documenting, testing, reviewing, and approving changes to information systems.	Inspected the Change Management Policy to determine that a Change Management Policy was documented and included guidance for documenting, testing, reviewing, and approving changes to information systems.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-54	Access to migrate changes to production is restricted to authorized personnel.	Inspected the system access listings, inquired of management, and compared each user's access privileges to their job role to determine that access to migrate changes to production was restricted to authorized personnel.	No exceptions noted.
REQ-55	Changes to software and infrastructure components are authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the change request tickets for a sample of software and infrastructure changes to determine that changes to software and infrastructure components were authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
REQ-56	System changes are communicated to authorized internal users.	Inspected the change request tickets for a sample of system changes to determine that system changes were communicated to authorized internal users.	No exceptions noted.
REQ-57	Branch protection rules are configured in the development tool to help ensure code quality, prevent accidental or malicious changes, enforce security and compliance requirements, and maintain the stability of critical branches.	Inspected the branch protection rule configurations to determine that branch protection rules were configured in the development tool to help ensure code quality, prevent accidental or malicious changes, enforce security and compliance requirements, and maintain the stability of critical branches.	No exceptions noted.
REQ-58	A business continuity and disaster recovery (BC/DR) plan is documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	Inspected the BC/DR plan to determine that a BC/DR plan was documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-59	The BC/DR plan is tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	Inspected the BC/DR plan test results to determine that the BC/DR plan was tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	No exceptions noted.
REQ-60	A Data Backup and Recovery Policy is documented and includes guidance for the Company's data backup and recovery strategy.	Inspected the Data Backup and Recovery Policy to determine that a Data Backup and Recovery Policy was documented and included guidance for the Company's data backup and recovery strategy.	No exceptions noted.
REQ-61	Data backup restoration tests are performed annually to verify data recoverability.	Inspected the data backup restoration test results to determine that data backup restoration tests were performed annually to verify data recoverability.	No exceptions noted.
REQ-62	Daily backups are configured for databases housing customer data.	Inspected the backup configurations to determine that daily backups were configured for databases housing customer data.	No exceptions noted.
REQ-64	System capacity is evaluated continuously to help ensure that processing capacity can meet demand.	Inspected the system capacity monitoring tool dashboard, configurations and metrics to determine that system capacity was evaluated continuously to help ensure that processing capacity could meet demand.	No exceptions noted.
REQ-65	A Data Classification Policy is documented and includes guidance for the classification and security of confidential data.	Inspected the Data Classification Policy to determine that a Data Classification Policy was documented and included guidance for the classification and security of confidential data.	No exceptions noted.
REQ-66	Customer data is prohibited by policy from being used or stored in non-production systems or environments.	Inspected the Information Security Policy to determine that customer data was prohibited by policy from being used or stored in non-production systems or environments.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-67	Customer data is purged from the application environment upon customer request.	Inspected the data removal tickets for a sample of customers that requested data deletion to determine that customer data was purged from the application environment upon customer request.	No exceptions noted.

SECTION 5

Other Information

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

The information included in this section is presented by Patchworks' management to provide additional information and is not a part of Patchworks' description of its Patchworks Platform made available to user entities throughout the period August 1, 2025 to July 31, 2026. Information included in Patchworks' management response to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Control #	Results of Tests	Management's Response
REQ-29	Exceptions noted. For 1 of 1 sampled semi-annual periods, an access review was not completed.	Management acknowledges that an access review was not completed in accordance with the required frequency during the audit period. In response to this exception, management conducted a review of system access and confirmed that user access remained appropriate based on role and responsibility. No instances of unauthorized or excessive access were identified. The Company also maintains compensating controls — such as role-based access provisioning, termination procedures, and continuous access monitoring — which helped mitigate the risk during the period in which the review did not occur. To prevent recurrence, management has implemented a centralized tracking process and automated reminders to enforce timely completion of access reviews. Relevant personnel have been retrained on their responsibilities, and periodic audits have been introduced to verify compliance with the updated procedures going forward.

Control #	Results of Tests	Management's Response
REQ-44 & REQ-45	Exceptions noted. An annual penetration test was not conducted during the audit period.	Management acknowledges that a penetration test of the production environment was not conducted during the audit period. While the penetration test was not conducted, the Company maintained a robust vulnerability management program throughout the period, including regularly scheduled vulnerability scans, continuous security monitoring, endpoint protections, and a formal process to assess and remediate critical and high-risk vulnerabilities. These compensating controls helped mitigate the risks typically addressed by penetration testing. In response to this exception, a formal third-party penetration test was conducted to evaluate the security posture of the production environment. The results were reviewed, and identified findings were addressed or documented with appropriate risk treatment. To reduce the likelihood of recurrence, management has updated its security testing and governance procedures to ensure that penetration tests are scheduled, tracked, and completed in accordance with policy. A compliance calendar has been implemented, relevant personnel have been assigned ownership, and oversight mechanisms have been introduced to verify timely execution going forward.