minware

SOC 2 Type II Report

Report on minware's Description of its Software Development Intelligence System and on the Suitability of the Design and Operating Effectiveness of Its Controls Related to Security Throughout the Period

October 1, 2024 to September 30, 2025

CBIZ CPAs

TABLE OF CONTENTS

Acronym Table

AICPA	American Institute of Certified Public Accountants
AWS	Amazon Web Services
BoD	Board of Directors
CD	Continuous Development
CEO	Chief Executive Officer
CI	Continuous Integration
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DB	Database
DC	Description Criteria
ECS	Elastic Container Service
HR	Human Resources
IAC	Infrastructure as Code
IPE	Information Provided by the Entity
ISSC	Information Security Steering Committee
IT	Information Technology
MFA	Multi-Factor Authentication
minware	minware, Inc.
NDA	Non-Disclosure Agreement
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SOC	System and Organization Controls
SSH	Secure Shell
TLS	Transport Layer Security
TSC	Trust Service Criteria
TSP	Trust Service Principles
WAF	Web Application Firewall

Section 1

Assertion of minware's Management

minware.

Assertion of minware's Management

We have prepared the accompanying description of minware's Software Development Intelligence System titled "minware's Description of its Software Development Intelligence System" throughout the period October 1, 2024 to September 30, 2025, (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria)* (description criteria). The description is intended to provide report users with information about the Software Development Intelligence System that may be useful when assessing the risks arising from interactions with minware's system, particularly information about system controls that minware 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 (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*.

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

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

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

a. The description presents minware's Software Development Intelligence System that was designed and implemented throughout the period October 1, 2024 to September 30, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that minware's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of minware's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that minware's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of minware's controls operated effectively throughout that period.

d. The controls designed to address trust services criteria CC6.5 did not operate because the circumstances that warranted the operation of those controls did not occur during the period October 1, 2024 to September 30, 2025.

/s/ minware

Section 2

Independent Service Auditors' Report

Independent Service Auditors' Report

To: Management of minware

Scope

We have examined minware's accompanying description of its Software Development Intelligence System titled "minware's Description of its Software Development Intelligence System" throughout the period October 1, 2024 to September 30, 2025 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that minware's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at minware, to achieve minware's service commitments and system requirements based on the applicable trust services criteria. The description presents minware's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of minware's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

minware 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 minware's service commitments and system requirements were achieved. minware has provided the accompanying assertion titled "Assertion of minware's Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. minware 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 Auditors' 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 AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 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.

Emphasis of Matter

As noted in Section 4, there are certain controls that did not operate because the circumstances that warranted the operation of those controls did not occur. Therefore, we did not test the operating effectiveness of those controls as evaluated using trust services criteria CC6.5.

Opinion

In our opinion in all material respects:

a. The description presents minware's Software Development Intelligence System that was designed and implemented throughout the period October 1, 2024 to September 30, 2025 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period October 1, 2024 to September 30, 2025 to provide reasonable assurance that minware's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of minware's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period October 1, 2024 to September 30, 2025 to provide reasonable assurance that minware's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of minware's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of minware, user entities of minware's Software Development Intelligence System during some or all of the period October 1, 2024 to September 30, 2025, business partners of minware subject to risks arising from interactions with the Software Development Intelligence System, 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 complementary user entity 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 the specified parties.

CBIZ CPAs

CBIZ CPAs P.C.

Tampa, FL
December 1, 2025

Section 3

minware's Description of its
Software Development Intelligence System

Purpose and Scope of Report

This report is intended to provide report users with information about the service organization's system relevant to security to enable such users to assess and address the risks that arise from their relationships with the service organization. This description is intended to focus on the internal control structure of minware that is relevant to only users of its Software Development Intelligence System and does not encompass all aspects of the services provided or procedures followed by minware.

System Description

Company Overview and Services Provided

minware is an all-remote SaaS service company that analyzes data from version control, ticketing systems, and calendars to provide insights about software engineering productivity.

minware's goal is to help organizations consistently follow best practices used by top-performing teams by providing a step-by-step scorecard and tracking the impact of improvements on productive engineering time. minware tracks best practices across the entire software development lifecycle, from basic ticketing and version control hygiene to predictable sprints, roadmap delivery, and quality.

minware's time model precisely allocates work time to commit activity. It works by dynamically creating a schedule for each author based on their history, and then allocating active work time between commits to the commit that follows.

Principal Service Commitments and System Requirements

minware designs its processes and procedures related to its Software Development Intelligence System to meet its objectives. Those objectives are based on the service commitments that minware makes to user entities, the laws and regulations that govern service providers, and the financial, operational, and compliance requirements that minware has established for the services.

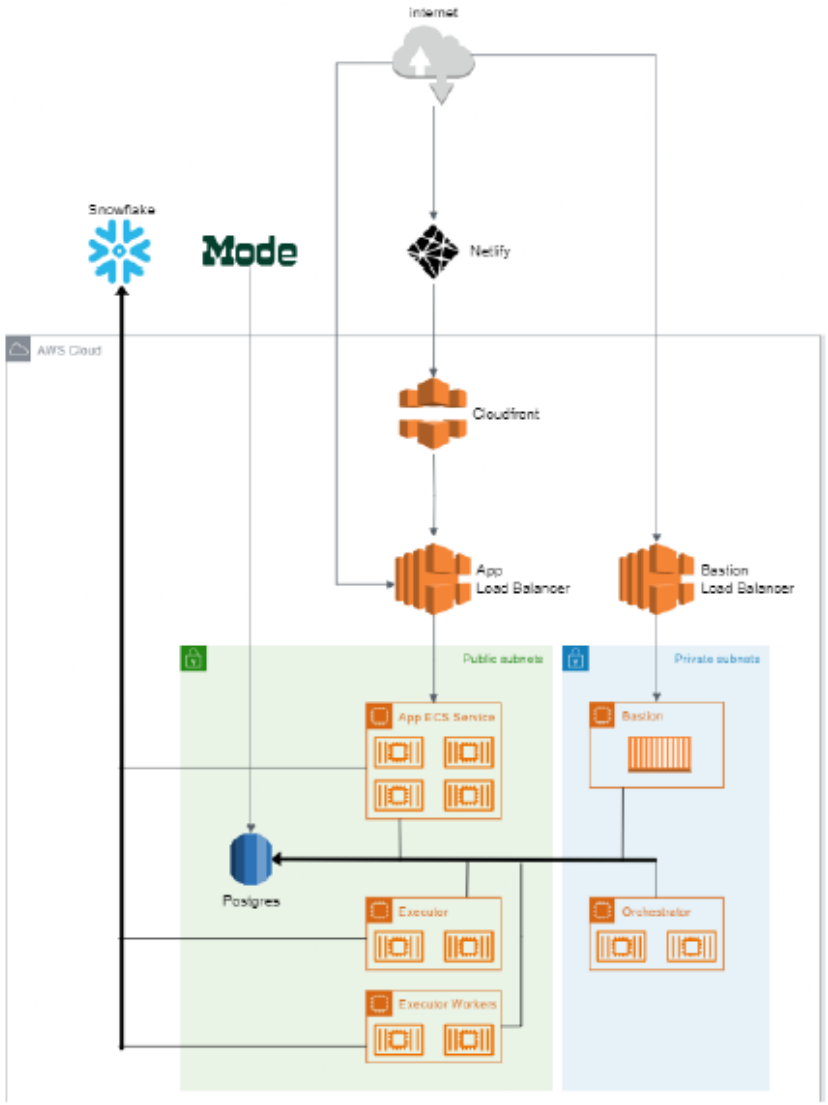
Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Software Development Intelligence System that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect client data at rest and in transit.
- Security of systems services and system components on AWS and Snowflake.
- Monitoring of subservice organizations' controls including AWS and Snowflake.

Infrastructure

The minware Software Development Intelligence System's infrastructure is hosted on the AWS cloud platform and uses Snowflake for its data warehousing. Security within the Software Development Intelligence System is addressed by a combination of AWS security groups, MFA, and secure SSH protocol tunneled access through a bastion host on an EC2 instance. Access to the Postgres database is fortified through the use of SSH tunnels that pass through a dedicated bastion host. The SSH tunnel employs encryption, safeguarding data in transit and providing secure remote access. With the bastion host acting as a single-entry point for SSH connections, it becomes easier to monitor and manage access, allowing system

administrators to enforce strict security policies and maintain a high level of data protection within the AWS-hosted architecture.



Software

The following provides a summary of the software and related services used in the delivery of the Software Development Intelligence System:

- Jira – help desk ticketing, project management, and workflow of alarm configurations to automatically generate a ticket for tracking and resolution.
- GitHub – version control software and CI/CD platform.
- Snowflake – data warehousing solution.
- AWS – cloud infrastructure services.
- CloudWatch – monitoring and logging of the cloud infrastructure.
- GuardDuty – threat detection service monitoring cloud infrastructure.

- Netlify – composable platform used to build and deploy serverless backend services.
- NEXT.js with React – for the presentation layer of their Web Interface and backend systems.
- Linux – for the bastion host.
- Mode – business intelligence tool.
- New Relic – application performance monitoring and logging tool.
- AWS Inspector – vulnerability management service scanning cloud applications settings and configurations.
- Opsgenie – manage and centralize system monitoring alerts.
- SendGrid – for e-mail notifications.
- Auth0 – authentication and authorization services to the application.
- Slack – business communication platform throughout the organization.
- AWS Secrets Manager – manage, retrieve, and rotate secrets and keys.
- Bitwarden – password management services.
- AWS ECS – compute services used for scheduled compute jobs.
- AWS Lambda – serverless compute services for on-demand processing jobs.
- Terraform – IAC tool used to automate infrastructure tasks.
- Docker – deployment of applications inside containers.
- Postgres DB – database management system.
- PopSQL – business intelligence tool.
- Stripe – payment processing platform.
- S3 – storage services.
- Mixpanel – tracking and logging user activities.
- Google Workspace – productivity apps (Gmail, Drive, Docs, etc.).
- Dropbox – file storage.

People

People involved in the operation and use of the system are:

- CEO – Responsible for the general oversight of the company and overall business strategy.
- Information Security Steering Committee (ISSC) – Responsible for ensuring the operational effectiveness of the Information Security Policy and all other associated policies and procedures.
- Principal Security Engineer – Responsible for all aspects of the system and application security engineering, conceptualizing and management of projects, and managing technical security risks.
- Employees and Contractors – Responsible for upholding security practices and following company policies and procedures.

Procedures

Executive Management personnel maintain documented automated and manual standard procedures involved in operation of Software Development Intelligence System that include:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication

- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- system and Information Integrity
- System and Services Acquisition

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which minware strives to achieve its business objectives. minware has applied a risk management approach to the organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

The minware control procedures, which have been designed to meet the applicable trust services criteria, are included in Section 4 of this report to eliminate the redundancy that would result from listing the procedures in this section as well.

Data

minware ingests data nightly from customer version control, ticketing, and calendar systems to provide insights around a company's software engineering productivity. Customers' systems are integrated into the data warehouse, Snowflake. Once integrated, the data is loaded and transformed by the application, which queries in Snowflake and displays the following types of reports within the web application:

- Custom Reports and Dashboards – Allow the user to define custom metrics and reporting based on the underlying software development data sources.
- Time Allocation – Provides a high-level view of how people spend their time and whether that time was used productively.
- Sprint Trends – Shows how tasks flow through sprints based on their estimates and illustrates trends in delivery vs. commitments.
- Scorecard – Provides a comprehensive list of how well people follow best practices across all layers of the productivity stack with specific, actionable insights about the most important areas to improve.
- Sprint Insights – Shows a detailed breakdown of all the activity that occurred during a particular sprint, both from a time and ticket/point perspective. This report is designed for teams to use during sprint retrospectives.

Data in transit is protected by employing secure and encrypted communication channels. Specifically, data transfers are safeguarded using the TLS protocol, which ensures that any data moving between the minware and client environments remains encrypted and inaccessible to unauthorized entities. This encryption

mechanism is crucial for maintaining the confidentiality and integrity of the data as it traverses potentially vulnerable networks.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Significant Changes to the System

There were no significant changes to the Software Development Intelligence System throughout the period.

Subservice Organizations

Amazon Web Services

minware uses AWS for hosting production systems. AWS is responsible for the uptime, management, physical and logical security of the infrastructure that supports the delivery of internet, and environmental conditions that provide power and cooling to their devices. AWS is also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

On an annual basis, minware obtains a third-party SOC 2 Type II report from AWS and reviews the report and testing results to determine if there were appropriate controls in place, and that they were operating effectively. In the event that there are exceptions or controls not operating effectively at AWS, this risk is incorporated into a risk assessment and appropriate actions are taken to mitigate future risks.

The applicable trust services criteria that are intended to be met by controls at AWS, alone or in combination with controls at minware, and the types of controls expected to be implemented at AWS to meet those criteria are described in the section below:

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2
AWS is responsible for restricting logical and physical access to their facilities and system components including firewalls, routers, and servers.	CC6.1, CC6.2, CC6.4, CC6.5
AWS is responsible for maintaining segregation of minware's environment(s) from other AWS clients.	CC6.1, CC6.6
AWS is responsible for securely disposing of hosted physical assets once they have reached end-of-life.	CC6.5
AWS is responsible for the management of any third-party vendors with access to customer environments.	CC9.2

Snowflake

minware uses Snowflake for cloud-based data warehousing that manages the storage, retrieval, and analysis of data. Snowflake is responsible for maintaining the integrity and security of the data, facilitating scalable and elastic data operations that can adapt to changing workloads. Additionally, Snowflake is tasked with compliance management, adhering to industry standards and regulations to ensure that data handling meets the required security benchmarks. It supports the SaaS company's analytics and data-driven decision-making by offering a reliable and efficient data warehousing service.

On an annual basis, minware obtains a third-party SOC 2 Type II report from Snowflake and reviews the report and testing results to determine if there were appropriate controls in place, and that they were operating effectively. In the event that there are exceptions or controls not operating effectively at Snowflake, this risk is incorporated into a risk assessment and appropriate actions are taken to mitigate future risks.

The applicable trust services criteria that are intended to be met by controls at Snowflake, alone or in combination with controls at minware, and the types of controls expected to be implemented at Snowflake to meet those criteria are described in the section below:

Control Activities Expected to be Implemented by Snowflake	Applicable Trust Services Criteria
Snowflake is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2
Snowflake is responsible for maintaining segregation of minware and minware client environments from other Snowflake clients.	CC6.1, CC6.6
Snowflake is responsible for the management of any third party vendors with access to customer environments.	CC9.2
Snowflake is responsible for limiting access to information systems and data through user authentication and authorization.	CC6.1, CC6.2
Snowflake is responsible for utilizing firewalls, intrusion detection systems, and other measures to prevent unauthorized access.	CC6.1, CC6.2, CC6.3, CC6.6
Snowflake is responsible for maintaining comprehensive information security policies that are communicated to and acknowledged by employees.	CC1.1
Snowflake is responsible for implementing formal processes to manage changes to system software and configurations.	CC8.1
Snowflake is responsible for securing facilities with controls such as badge access, surveillance cameras, and environmental protections.	CC6.4

Control Environment

Control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Below are the key areas and the description of controls that support minware's control environment.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how those standards are communicated, and how they are reinforced in practice. Behavioral standards could include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts and the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership's example.

minware has implemented, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior. minware's management conducts business dealings with employees, suppliers, customers, and auditors on a high ethical plane and insists others have similar business practices.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

minware assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job. minware reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions for the security of information. minware's management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Organizational Structure

An entity's organizational structure provides the framework for how company-wide objectives are planned, executed, controlled, and monitored. A relevant organizational structure includes considering key areas of authority and responsibility, as well as appropriate lines of reporting. An entity develops an organizational structure contingent, in part, on its size and nature of activities.

The responsibilities of key positions within minware are clearly defined and communicated. Individuals that hold key positions are experienced, knowledgeable, and have lengthy tenure and experience within the given fields of their roles and responsibilities at minware. minware's organizational structure supports

communication of information both up to leadership as well as down to support staff, ensuring clear and effective communication channels. minware's organizational structure is comprised of six primary business units that work together to deliver the Software Development Intelligence System.

The business units consist of:

- Executive Management - Responsible for providing execution of business objectives and strategic direction.
- Finance Team – Responsible for managing financial operations and ensuring compliance with regulations.
- Marketing Team – Responsible for developing and implementing marketing strategies to generate leads and support sales.
- Customer Support and Success Team – Responsible for providing technical support and building customer relationships to improve product success.
- Sales Team – Responsible for identifying and pursuing sales opportunities to achieve revenue goals.
- Product and Development Team – Responsible for designing, developing, and implementing software products to ensure their success.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions, and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge, and experience required of key personnel and the appropriate number of people to carry out duties. In addition, management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

As mentioned above, minware has defined job responsibilities and clear communication channels to disseminate information within the organization; this enables minware to react to market and regulation changes and to meet its goals and objectives. minware is appropriately staffed to support its operations, particularly with respect to critical areas such as software development, implementation, customer support, and IT system support.

HR Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counseling, and remedial action. Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior demonstrate minware's commitment to hiring and retaining only highly competent and trustworthy people. Personnel career growth and reward of meeting expectations are driven by periodic performance feedback and demonstrate minware's commitment to advance qualified personnel to higher levels of responsibility. Personnel who

work for minware are required to read and acknowledge the company's internal policies and confidentiality requirements as well as the confidentiality of customer managed information.

Risk Assessment

minware management performs an annual risk assessment, which requires management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. minware's management reevaluates the risk assessment annually or when otherwise necessary to both update the previous results and to identify new areas of concern.

The risk assessment process consists of the following phases:

- Identifying: The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing: The assessment phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence.
- Mitigating: The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Reporting: The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and applicable regulations.
- Monitoring: The monitoring phase includes minware management performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

Consideration of Fraud

Risks of fraudulent activities being carried out are addressed in the risk assessment and the treatment process described above by the risk management team. This process is aimed to identify and address the company's vulnerabilities to internal and external fraud.

In-Scope Trust Service Categories

The table below provides the TSC within the scope of this report. The controls designed and implemented to meet the applicable TSC criteria have been included in Section 4.

Trust Services Category	Definition
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the security of information or systems and affect the entity's ability to meet its objectives.

Security

Security refers to the protection of

- Information during its collection or creation, use, processing, transmission, and storage.
- Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other

unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust Service Categories and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, minware has identified, and put into place, the necessary actions to address those risks and help ensure competent and efficient operations. Control activities serve as mechanisms for managing the achievement of the security principle and applicable criteria.

Selection and Development of Control Activities

The applicable TSC and related control activities are included in the control matrices, within Section 4 of this report, to eliminate the redundancy that would result from listing the items in this section as well. Although the control activities are included in the testing matrices set forth below in Section 4, they are, nevertheless, an integral part of minware's description of its Software Development Intelligence System. Any applicable TSC that are not addressed by control activities at minware are also described within the control matrices.

Information and Communication

Information

Information is necessary for minware to carry out internal control responsibilities to support the achievement of its objective related to the Software Development Intelligence System. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

The following provides a summary of internal and external sources of information used in the Software Development Intelligence System:

- Third party vendor attestation reports are obtained and reviewed, and remediation plans are proposed and monitored through resolution.
- Release notes are communicated to internal system users for system changes, maintenance, and upgrades that affect system security and functionality.
- Annual penetration tests are performed, and remediation plans are documented and tracked until resolved.
- System change management activities (e.g. development efforts, testing, peer review, approvals, etc.) are documented within Jira.
- Security events are documented, tracked, resolved, and communicated to all affected parties.
- Enterprise monitoring statistics (e.g. performance, availability, utilization, and capacity levels) are monitored using CloudWatch and New Relic.

Communication

Throughout the organization, minware conducts monthly and quarterly meetings to identify and address significant issues affecting its operations. A defined agenda and corporate information system are used as established vehicles for addressing and monitoring activities, accomplishments, and issues. A monthly management meeting provides the vehicle for Executive Management to communicate and respond to

operational tasks and issues. The minware BoD meets regularly to discuss internal controls, operations, and business objectives.

Internal Communications

minware has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events were communicated. These methods include orientation for new employees and ongoing trainings for employees. Job descriptions are provided to employees and evaluations are completed against those job descriptions annually.

External Communications

minware has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in communication of significant events. These methods include the use of e-mail messages and a customer contact option on the minware website.

Monitoring

Monitoring is generally performed through active, hands-on management, including regular management and BoD meetings. Management is involved and active in the business. minware utilizes a risk-based approach to monitor business units and other entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance. Results from the risk evaluation are documented in formal communications to management and other relevant parties.

minware monitors customer communications through the help desk ticketing system. This information is provided to the system administrators, providing the ability to track, monitor and assist in understanding customer complaints or concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor customers' communications is integral to controlling the quality of the services provided.

minware monitors customer communications and engagements through their customer support department. Client communications are received by the customer support department and are then disseminated throughout the minware organization.

Management strives to be proactive in responding to customer complaints and maintaining a high level of inter-departmental communication about these events. Customer complaints and other issues are handled via the customer support department.

Complementary User Entity Controls

The control activities performed by minware cover only a portion of the overall internal control structure of minware's user entities. Therefore, each customer's internal control structure must be evaluated in conjunction with minware's control policies and procedures described in this report. minware's controls over its Software Development Intelligence System were designed with the understanding that certain user entity controls were in place and operating effectively.

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for immediately notifying minware of any actual or suspected information security breaches, including compromised user accounts.	CC7.3

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for determining whether minware's security infrastructure is appropriate for its needs and for notifying the service organization of any requested modification.	CC6.1, CC6.2, CC6.3
User entities are responsible for notifying minware of any approved contract modifications.	CC6.2
User entities are responsible for ensuring that user IDs and passwords used for accessing minware systems are assigned only to authorized individuals and that the roles assigned to the user account are appropriate.	CC6.2
User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with minware's Software Development Intelligence System.	CC6.2
User entities are responsible for notifying minware of any changes to their confidentiality requirements and obtain approval in writing.	CC6.2

Section 4

Trust Services Category, Criteria,
Related Controls, and Tests of Controls

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by minware throughout the period of October 1, 2024 to September 30, 2025. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved throughout the period. The nature of the tests conducted took into consideration the type of control testing and the evidential matter that is available to perform a test to determine the operating effectiveness.

Procedures for Assessing Completeness and Accuracy of IPE

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

1. Inspect the source of the IPE
2. Inspect the query, script, or parameters used to generate the IPE
3. Tie data between the IPE and the source, and/or
4. Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Types of Tests Performed:

1. **Inquiry:** tests include the corroboration of relevant personnel to verify the knowledge and understanding of the described control activity.
2. **Observation:** tests include the physical observation of the implementation, application of, or existence of specific controls.
3. **Inspection:** tests include the physical validation of documents, records, configuration, or settings.
4. **Re-performance:** tests include the reprocessing of transactions, procedures, and calculations to ensure the accuracy and completeness of the control description.

Test	Description of Test
Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.
Observation	Observed application or existence of specific controls.
Inspection	Inspected documents and reports indicating performance of the control.
Reperformance	Reperformed the internal control procedures

Trust Services Category, Criteria, Related Controls, and Tests of Controls

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC1.0	**Control Environment**				
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	Employees are required to read and sign an acknowledgement form indicating that they have read, understand, and agree to adhere to the policies contained within the employee handbook.	Inspected the signed employee handbook for the only new hire to verify that employees signed an acknowledgment form stating they have read, understood, and agreed to the employee handbook policies.	No exceptions noted.
		CC1.1.2	Employees are required to read and sign a separate non-disclosure agreement.	Inspected the signed NDA for the only new hire to verify that employees signed a separate non-disclosure agreement.	No exceptions noted.
		CC1.1.3	Pre-employment screening procedures are in place to qualify candidates of their competency of the job requirements.	Inspected the onboarding process for the only new hire to verify that pre-employment screening procedures were in place to evaluate candidates' competency for the job requirements.	No exceptions noted.
		CC1.4.3 CC9.2.2 CC9.2.3	See CC1.4.3, CC9.2.2, and CC9.2.3.		
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1	An Information Security Policy is in place with defined oversight responsibilities and sufficient expertise and independence to perform its duties.	Inspected the information security policy to verify that the information security policy was in place with defined oversight responsibilities and sufficient expertise and independence to perform its duties.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	Each organizational unit is assigned responsibilities and authorities for the design, development, implementation, operation, maintenance and monitoring of the system to meet their commitments and requirements. An organizational chart with relevant reporting lines is documented and made available to personnel.	Inspected the organizational chart, where it was made available to users, and information security policy to verify that each unit’s assigned system responsibilities and authorities and was made available through the internal HR system.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC1.3.2	A primary point of contact within the organization is defined for external third parties and authorities/responsibilities are established.	Inspected the vendor tracking system for a sample of vendors to verify that a primary point of contact was in place for each vendor with an assigned owner defined.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.1	Senior management develop contingency plans for assignments of responsibility important for internal control.	Inspected the business continuity and disaster recovery plan and the contingency plan for key roles to verify that senior management developed contingency plans for the assignment of responsibilities important for internal control.	No exceptions noted.
		CC1.4.2	Employees are required to complete security awareness training upon hire and on an annual basis.	Inspected the security awareness training completion logs for a sample of newly hired and current employees to verify that training was completed upon hire and annually thereafter.	No exceptions noted.
		CC1.4.3	Performance evaluations are completed on an annual basis.	Inspected the completed performance review documentation for a sample of current employees to verify that performance evaluations were completed on an annual basis.	No exceptions noted.
		CC1.4.4	The company maintains job descriptions defining the competencies required within the organization and is reviewed on an annual basis and made available to personnel.	Inspected the company's job descriptions and its annual review to verify that job descriptions were established and defined the competency requirements for each role.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.5.1	Accountability for internal control is established, defined, assigned to the responsible parties, and evaluated at least annually by the security team to help ensure performance measures are met and corrective measures are implemented as needed.	Inspected the information security policy and internal control audit report to verify that accountability for internal control was established, defined, assigned to the responsible parties, and reviewed annually by the security team.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC1.5.2	Performance measures are defined across the organization to measure short and long term goals and measured/monitored at least annually.	Inspected the information security steering committee charter and meeting minutes to verify that performance measures were defined across the organization to measure short and long term goals and were measured/monitored at least annually.	No exceptions noted.
		CC1.4.3 CC1.4.4	See CC1.4.3 and CC1.4.4.		
CC2.0	**Communication and Information**				
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.1	Internal control practices and procedures are reviewed annually for applicability and improvement, including the data and data sources used to support them.	Inspected the internal audit procedures and information security policy to verify that internal control practices were reviewed annually for applicability and improvement, and included the data and data sources used to support them.	No exceptions noted.
		CC2.1.2	Management has identified the information needed to support the functioning of internal controls (i.e. reports, system results, internal or external testing, HR reports (e.g. training status, evaluation status, disciplinary etc., service level commitments reporting)).	Inspected the internal audit report to verify that management identified the information needed to support the functioning of internal controls.	No exceptions noted.
		CC2.1.3	Monitoring of the required information is reviewed by management on an annual basis to ensure information is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	Inspected the internal audit report and evidence of the review and approval of results by the information security steering committee to verify that management was responsible for monitoring of the required information on an annual basis to ensure that information was timely, current, accurate, complete, accessible, protected, verifiable, and retained.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.2.1	A management review of information regarding the functioning of internal control is documented with action plans as needed as a result of the review. Results of the internal review are communicated to the executive committee.	Inspected the internal audit process review, internal audit report, and the information security steering committee meeting minutes to verify that a management review of information regarding the functioning of internal control was documented and communicated to executive committee during the information security steering committee meeting.	No exceptions noted.
		CC2.2.2	Results of internal monitoring procedures are communicated to impacted departments or personnel.	Inspected the internal audit report and the information security steering committee meeting minutes to verify that the findings of internal monitoring procedures were conveyed to relevant departments or personnel.	No exceptions noted.
		CC2.2.3	Changes to internal control activities are required to be approved by the authorized organizational unit and communicated to relevant personnel.	Inspected the information security policy to verify that changes to internal control activities were required to be approved by the authorized organizational unit and communicated to relevant personnel. Inspected the list of internal control changes to verify that no internal control changes occurred during the period.	Control did not operate - No internal control changes occurred throughout the period to test the operating effectiveness of the control activity.
		CC2.2.4	All users of the system are provided with information on how and where to report issues (i.e. failures, incidents, concerns, or complaints) related to the system.	Inspected the incident response plan, information response policy, contact page on the company website, and email notification from the contact page to verify that all users of the system were provided with information on how and where to report issues related to the system.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.1	Material changes to nondisclosure agreements or other contractual confidentiality provisions are required to be communicated and affirmed by the business partner or third party vendor prior to contract renewal.	Inspected the nondisclosure agreement template to verify that an NDA template was in place and dictated that any material modifications to the terms were required to be communicated and approved prior to enforcing. Inquired of the CEO to verify that there were no recent NDA's executed or modifications to the confidentiality provisions during the period.	Control did not operate - No material changes to nondisclosure agreements or other contractual confidentiality provisions occurred to test the operating effectiveness of this control activity.
		CC2.3.2	Changes to internal control activities impacting external parties are communicated to relevant users of the system.	Inspected the information security policy to verify that changes to internal control activities impacting external parties were required to be communicated to relevant users of the system. Inspected the list of internal control changes to verify that no internal control changes occurred during the period.	Control did not operate - No changes to internal control activities occurred to test the operating effectiveness of this control activity.
		CC2.2.4	See CC2.2.4.		
CC3.0	**Risk Assessment**				
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.1	A risk assessment policy defines management's overall objectives as it relates to relevant risk internal and external. The risk assessment policy is reviewed annually or upon a significant event that would require additional evaluation.	Inspected the risk assessment policy to verify that the policy defined management's overall objectives as it related to relevant risk internal and external, and that the policy was reviewed annually or upon a significant event that would require additional evaluation.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC3.2.1	Risk assessments are performed annually and upon implementation of any new technology that could impact the system and commitments. The risk assessment includes the analysis of threats and vulnerabilities to the system, ranks threats and vulnerabilities based of the level of risk, and management determines risk acceptance or mitigation action plans as a part of the overall risk assessment.	Inspected the risk assessment report to verify that a risk assessment was performed on an annual basis or upon implementation of new technology to analyze, rank, and determine acceptance or mitigation strategies for identified risks to the organization.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.3.1	The risk assessment includes the consideration for fraud.	Inspected the risk assessment report to verify that the risk assessment included the consideration for fraud.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.4.1	As part of the risk assessment, risk identification includes addressing on-going changes throughout the organization and defines authorization, communication, and reporting of changes to those activities. The entity identifies and assesses the following changes that could significantly impact the system of internal control including: ➢ External environment ➢ Current business model ➢ Leadership ➢ Technology ➢ Business relationships (vendors, business partners, other third parties)	Inspected the risk assessment report to verify that the following topics were identified and assessed by management: ➢ External environment ➢ Current business model ➢ Leadership ➢ Technology ➢ Business relationships (vendors, business partners, other third parties)	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC4.0	**Monitoring Activities**				
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC4.1.1	An internal control monitoring program is put in place to ensure that controls are designed and operating as intended. Identified issues are assessed and action plans defined and monitored until implemented.	Inspected the information security policy, internal audit report, and the control tracking review to verify that an internal control monitoring program was in place to ensure controls were designed and operating as intended, and that identified issues were assessed and action plans defined and monitored until implemented.	No exceptions noted.
		CC4.1.2	Monitoring systems are utilized to monitor system performance and notify personnel of system errors and unusual activity.	Inspected the cloud monitoring tool, monitoring alert settings, monitoring review, and most recent alerts received to verify that monitoring systems were utilized to monitor system performance and notify personnel of system errors and unusual activity.	No exceptions noted.
		CC4.1.3	An annual penetration test is performed to identify that the design of security controls are operating as intended. Results of this assessment are reviewed and approved by management. Corrective actions plans are created and tracked when necessary.	Inspected the penetration test report to verify that an annual penetration test was performed to ensure the design of their security controls were operating as intended, and no corrective actions were needed.	No exceptions noted.
		CC4.1.4	Code reviews are performed to ensure software development activities are following the design of their coding practices.	Inspected the secure software development lifecycle policy and the pull requests for a sample of system changes to verify that code reviews were performed to ensure development activities were following the design of their coding practices.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CC4.2.1	Control failures and deficiencies, and proposed corrective action plans for newly identified issues, are communicated to management based on the type of control failure. Deficiencies are assessed and corrective action are tracked for timely completion.	Inspected the internal audit report and the most recent ISSC meeting minutes to verify that control failures and deficiencies would be reported to management, corrective action plans proposed, and deficiencies assessed and tracked for timely resolution. Inspected the control tracking instances to verify that there were no internal control changes.	Control did not operate - No changes to internal control activities occurred to test the operating effectiveness of this control activity.
		CC4.1.3	See CC4.1.3.		
CC5.0	**Control Activities**				
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.1	The information security policy is required to be reviewed and approved by management and communicated throughout the organization at least annually.	Inspected the information security policy and mass email communication to all employees to verify that the information security policy was reviewed and approved by management and communicated throughout the organization at least annually.	No exceptions noted.
		CC5.1.2	As a result of the risk assessment process a risk treatment plan is created to identify and/or implement controls to support the achievement of management objectives for identified risks.	Inspected the risk assessment report to verify that the risk assessment process included a risk treatment plan to identify controls to support the achievement of managements objectives for identified risks.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC5.1.2	See CC5.1.2		

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC5.3.1	Policies and procedures are in place that address: ➢ Access control ➢ Audit and accountability ➢ Awareness and training ➢ Configuration management ➢ Contingency planning ➢ Identification and authentication ➢ Incident response ➢ Maintenance ➢ Media protection ➢ Personnel security ➢ Physical protection ➢ Risk assessment ➢ Security assessment and authorization ➢ System and services acquisition ➢ System and communications protection ➢ System and information integrity	Inspected the information security policy to verify that policies and procedures were in place that addressed: ➢ Access control ➢ Audit and accountability ➢ Awareness and training ➢ Configuration management ➢ Contingency planning ➢ Identification and authentication ➢ Incident response ➢ Maintenance ➢ Media protection ➢ Personnel security ➢ Physical protection ➢ Risk assessment ➢ Security assessment and authorization ➢ System and services acquisition ➢ System and communications protection ➢ System and information integrity	No exceptions noted.
CC6.0	**Logical and Physical Access Controls**				
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.1	An inventory of information assets is maintained, and each type of asset is classified based on the information asset classification policy.	Inspected the data classification and handling policy and the inventory of information assets to verify that an inventory of information assets was maintained, and each type of asset was classified based on the information asset classification policy.	No exceptions noted.
		CC6.1.2	A network diagram is documented and reviewed annually to ensure it accurately reflects the current network architecture.	Inspected the network diagram to verify that a network diagram was documented and reviewed annually to ensure it accurately reflected the current network architecture.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC6.1.3	Multi factor and local user access permissions provide authentication, access restrictions, and prevention of unauthorized user access attempts to the AWS console and supporting resources (i.e. API's, Virtual Servers, Security Services).	Inspected the AWS authentication configurations and the list of AWS administrators to verify that MFA and local user access permissions provided authentication, access restrictions, and prevention of unauthorized user access attempts to the console and supporting resources.	No exceptions noted.
		CC6.1.4	AWS security groups are in place and configured to filter unauthorized inbound network traffic from the Internet.	Inspected the security group inbound rules to verify that AWS security groups were in place and configured to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		CC6.1.5	Access to modify AWS security groups is restricted to system administrators.	Inspected the list of users with access to modify AWS security groups and the user access review to verify that access to modify AWS security group was restricted to system administrators and was reviewed during the user access review.	No exceptions noted.
		CC6.1.6	Access to the database is restricted via security groups.	Inspected the AWS security group policy to verify that access to the database was restricted via security groups.	No exceptions noted.
		CC6.1.7	SSH keys are securely stored and rotated to maintain up-to-date keys and compromised keys are revoked.	Inspected the key rotation policy, key rotation settings, and the recently completed key rotation to verify that SSH keys were stored and rotated to maintain up to date keys and compromised key were revoked.	No exceptions noted.
		CC6.1.8	Encryption is utilized to protect data-at-rest.	Inspected the encryption configurations for sample of workstations, databases, and storage systems to verify that encryption was utilized to protect data-at-rest.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC6.1.9	Serverless functions that call out to a service require access control and authentication using the concept of least-privilege to prevent misuse.	Inspected the resource-based permissions assigned to the AWS lambda functions to verify that serverless functions that called out to a service required access control and authentication using the concept of least privilege.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.2.1	All system access for internal users is required to adhere to the user provisioning procedures which require formal documented authorization prior to granting access to system components and data.	Inspected the onboarding documentation for the only newly hired employee to verify that system access adhered to user provisioning procedures which required documented authorization before provisioning access.	No exceptions noted.
		CC6.2.2	User account access is revoked upon notification of termination.	Inspected the information security policy and offboarding process to verify that user access would be revoked upon termination notification. Inspected the list of employees to verify that there were no employees terminated during the period.	Control did not operate - No employee terminations occurred to test the operating effectiveness of this control activity.
		CC6.2.3	User access reviews are performed annually to validate accounts and permissions are assigned to authorized personnel.	Inspected the full system access review to verify that user access reviews were performed annually to validate accounts and permissions were assigned to authorized personnel.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC6.3.1	Administrative access to Auth0 is restricted to system administrators.	Inspected the list of users with administrative access to Auth0 and the user access review to verify that administrative access was restricted to authorized system administrators.	No exceptions noted.
		CC6.3.2	Administrative access to the data warehouse is restricted to appropriate personnel.	Inspected the list of users with administrative access to the data warehouse and the user access review to verify that access was restricted to appropriate personnel.	No exceptions noted.
		CC6.3.3.	Administrative access to GitHub is restricted to system administrators.	Inspected the list of users with administrative access to GitHub and the user access review to verify that administrative access was restricted to authorized system administrators.	No exceptions noted.
		CC6.3.4	Access to administer the permissions of serverless functions roles and groups is limited to authorized administrators.	Inspected the list of users within AWS to modify permission and the user access review to verify that access to administer the permissions of the serverless functions roles and groups were restricted authorized administrators and was reviewed during the user access review.	No exceptions noted.
		CC6.2.1 CC6.2.2 CC6.2.3	See CC6.2.1, CC6.2.2, and CC6.2.3.		

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			N/A - Physical security is the responsibility of the subservice organizations.	
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.1	Data disposal policies and procedures are in place to conform to confidentiality commitments and requirements.	Inspected the data destruction policy and procedure documentation and the asset disposal checklist to verify that disposal procedures were in place to conform to confidentiality requirements.	No exceptions noted.
		CC6.5.2	Data and software stored on equipment is confirmed to be removed and rendered unreadable prior to disposal.	Inspected the data destruction policy and decommission checklist to verify data and software were required to be removed and rendered unreadable prior to disposal. Inspected the re-purposed physical asset log to verify that there were no recently disposed assets to require removal of data and software.	Control did not operate - No physical assets disposals occurred to test the operating effectiveness of this control activity.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.1	An automated and continual vulnerability management tool is utilized to scan and assess the security of workloads for vulnerabilities.	Inspected the automated vulnerability scanning configurations, results, and alert integration configurations to verify that an automated and continual vulnerability management tool was used to scan and assess workloads for vulnerabilities.	No exceptions noted.
		CC6.6.2	Web application firewalls are utilized to prevent malicious attempts on web applications.	Inspected the web application firewall dashboard to verify that a WAF was utilized to prevent malicious attempts on web applications.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC6.6.3	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the TLS encryption settings for the public facing application to verify that secure data transmission protocols were used to encrypt confidential and sensitive data.	No exceptions noted.
		CC6.1.4 CC6.1.6	See CC6.1.4, and CC6.1.6.		
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.7.1	The company utilizes encryption on its mobile devices to ensure information is protected internally.	Inspected the disk encryption configurations enabled on a sample of workstations to verify that the company utilized encryption on its mobile devices to ensure information was protected internally.	No exceptions noted.
		CC6.1.4 CC6.1.6	See CC6.1.4, and CC6.1.6.		
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC6.8.1	Container images are scanned for vulnerabilities and updated with the latest security patches in a timely manner.	Inspected the system patching and updates tickets and the scanning configurations to verify that container images were scanned for vulnerabilities and updated with the latest security patches.	No exceptions noted.
		CC6.8.2	Antivirus and anti-malware software is implemented and maintained on workstations to provide for the interception or detection and remediation of malware.	Inspected the antivirus software enabled for a sample of workstations to verify that workstations utilized the built-in antivirus software to provide the interception or detection and remediation of malware.	No exceptions noted.
		CC6.8.3	Serverless function code repositories are scanned continuously to detect any vulnerabilities.	Inspected the vulnerability scanning tool to verify that serverless functions were scanned continuously to detect any vulnerabilities.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC7.0	**System Operations**				
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC7.1.1	Images are utilized for production servers and security reviews are completed for employee workstations to verify that standards were in place and required to be utilized when deploying new systems into production and systems were reviewed for appropriate configuration.	Inspected the infrastructure as code repository, workstation provisioning guide, and evidence of security reviews to verify that configuration standards were in place and utilized when deploying new systems into production, and systems were reviewed for appropriate configuration.	No exceptions noted.
		CC7.1.2	External vulnerability assessments are performed on the production network quarterly to identify potential vulnerabilities. Identified vulnerabilities are assessed and actions taken if required to remediate vulnerabilities.	Inspected a vulnerability scan report, review, and remediated tickets for a sample of quarters to verify that scanning was performed on production network to identify vulnerabilities, and identified vulnerabilities and actions were taken to remediate the vulnerabilities.	No exceptions noted.
		CC7.1.3	AWS Trusted Advisor is utilized to help identify potential misconfigurations	Inspected the AWS Trusted Advisor dashboard to verify that AWS Trusted Advisor was utilized to help identify potential misconfigurations.	No exceptions noted.
		CC4.1.3	See CC4.1.3.		
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CC7.2.1	System logging is monitoring containers, servers, and functions, and system logs are evaluated to identify and report unusual or malicious activities.	Inspected the logging source setting, event triggers, and notification settings to verify that system logging was enabled to monitor containers, servers, and functions, and that logs were evaluated to identify and report unusual or malicious activities.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC7.2.2	A threat detection system is in place that continuously monitors the cloud environment for malicious activity and unauthorized behavior.	Inspected the threat detection system configurations, log, and alert configurations to verify that a threat detection system was in place that continuously monitored the cloud environment for malicious activity and unauthorized behavior.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.3.1	Security incident and response procedures are defined and communicated to inform users on where to report suspected security issues.	Inspected the incident response plan and policy to verify that security incident response procedures were defined and communicated to inform users on where to report suspected security issues.	No exceptions noted.
		CC7.3.2	Reported security issues are required to be documented, assessed for the impact of the reported event, monitored until resolved, and post resolution the events are assessed to determine if actionable plans are needed going forward.	Inspected the incident response plan and policy to verify that reported security issues were required to be documented, assessed for impact of the reported event, monitored until resolved, and evaluated for future actions post-resolution, if applicable. Inspected the list of security incidents to verify that no security incidents occurred during the period.	Control did not operate - No security incidents occurred to test the operating effectiveness of this control activity.
		CC7.3.3	Annually a security incident response test is performed testing the effectiveness of their procedures.	Inspected the incident response tabletop exercise to verify that a security incident response test was performed annually, testing the effectiveness of their procedures.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC7.3.1 CC7.3.2 CC7.3.3	See CC7.3.1, CC7.3.2, and CC7.3.3		

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC7.3.1 CC7.3.2 CC7.3.3	See CC7.3.1, CC7.3.2, and CC7.3.3.		
CC8.0	**Change Management**				
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC8.1.1	The entity has adopted a formal systems development life cycle methodology that governs the development, implementation, and maintenance of computerized information systems and related technology. It includes the design, implementation, configuration, modification and management of infrastructure and software and is consistent with defined commitments.	Inspected the secure software development lifecycle policy to verify that the organization adopted the SDLC methodology that governed the development, implementation, and maintenance of computerized information systems.	No exceptions noted.
		CC8.1.2	The development platform is configured to notify system users of the latest modifications.	Inspected the instant message notifications for a sample of system changes to verify that the development platform was configured to notify users of the latest modifications.	No exceptions noted.
		CC8.1.3	Change requests are documented and evaluated for business justification, prioritized, and require management's approval prior to development.	Inspected the change documentation for a sample of system changes to verify that change requests were documented and evaluated for business justification, prioritized, and required management's approval prior to development.	No exceptions noted.
		CC8.1.4	New system development projects and enhancements require a formal feature requirements document that is reviewed and approved by management.	Inspected the technical planning documents for a sample of new systems to verify that new system development projects and enhancements required a formal feature requirements document that was reviewed and approved by management.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC8.1.5	Access to deploy change to production is restricted to authorized system administrators.	Inspected the list of users and permissions with access to deploy changes to production and the user access review to verify that access was restricted to authorized system administrators and was reviewed as a part of the user access review.	No exceptions noted.
		CC8.1.6	Deficiencies in system operations are reported as bugs and tracked via the change management software.	Inspected the ticket resolution status for a sample of bugs to verify that deficiencies in system operations were reported as bugs and tracked via the change management software.	No exceptions noted.
		CC8.1.7	Emergency changes are required to retroactively follow the standard change control process.	Inspected the SDLC policy and a pull request for a sample of emergency changes to verify that emergency changes adhered to the standard change control procedures outlined in the policy.	No exceptions noted.
		CC8.1.8	Confidential and personal data is not utilized in development and testing environments unless prior authorization is provided.	Inspected the production and test environments to verify that separate environments were utilized. Inspected the data within the test databases to verify that confidential and personal data was utilized in the testing environments.	No exceptions noted.
		CC7.1.1	See CC7.1.1		
CC9.0	**Risk Mitigation**				
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1.1	The application is constantly monitored to ensure uptime and the production datastore is configured to auto-scale to ensure that demand is being met.	Inspected the application monitoring dashboard, alerting configurations, and the production datastore auto-scaling settings to verify that the application was constantly monitored for uptime, and the production datastore was configured to auto-scale.	No exceptions noted.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC3.2.1 CC3.4.1 CC4.1.1	See CC3.2.1, CC3.4.1, and CC4.1.1.		
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CC9.2.1	Documented policies and procedures are in place that define requirements for managing vendor and business partner relationships, including: 1) Defining a responsible individual or department for managing vendor relationships and reviews (including security risks to the Organization). 2) Defining a communication path with a vendor and having key contact and emergency handling information available.	Inspected the third-party vendor management policy and the vendor tracking table to verify that documented policies and procedures were in place that defined requirements for managing vendor and business partner relationships, and included the individual responsible for managing vendor relationships and defined a communication path with vendors and the point of contact.	No exceptions noted.
		CC9.2.2	High-risk vendor systems are subject to review as part of the vendor risk management process. Attestation reports are obtained and evaluated when available.	Inspected the vendor management policy and the vendor security review forms for a sample of critical vendors to verify that high-risk vendors were subject to review and attestation reports were obtained and evaluated.	No exceptions noted.
		CC9.2.3	Exceptions identified in the vendor review process are reviewed by management, discussed with the vendor, and a defined remediation plan is implemented, if necessary.	Inspected the vendor management policy to verify that exceptions identified in the vendor review process would to be reviewed by management, discussed with the vendor, and a defined remediation plan was implemented, if necessary. Inspected the vendor assessment documentation for a sample of critical vendors to verify that no exceptions were identified during the vendor review process to necessitate the review and implementation corrective actions.	Control did not operate - No exceptions identified during the vendor review process to test the operating effectiveness of this control activity.

Criteria #	Criteria	Control #	Control Activity Specified by the Service Organization	Test Applied by the Independent Service Auditor	Test Results
		CC9.2.4	Confidential data is confirmed to be removed from vendor systems upon termination of relationship.	Inspected the information security policy to verify that confidential data would be required to be removed prior to vendor systems upon termination of the relationship. Inspected the vendor listing to verify that there were no terminated vendors the occurred during the period.	Control did not operate - No vendor relationship terminations occurred to test the operating effectiveness of this control activity.