JOHANSON GROUP

System and Organization Controls (SOC) 2 Type II Report

Report on Controls Placed in Operation and Test of Operating Effectiveness Relevant to the Trust Services Criteria for Security Category

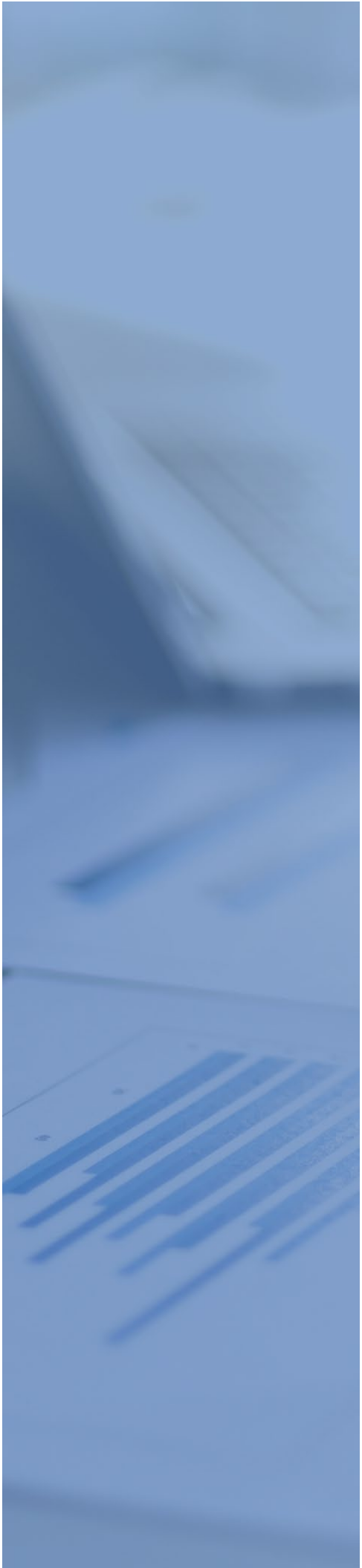
For the Period
June 19, 2023 to September 19, 2023

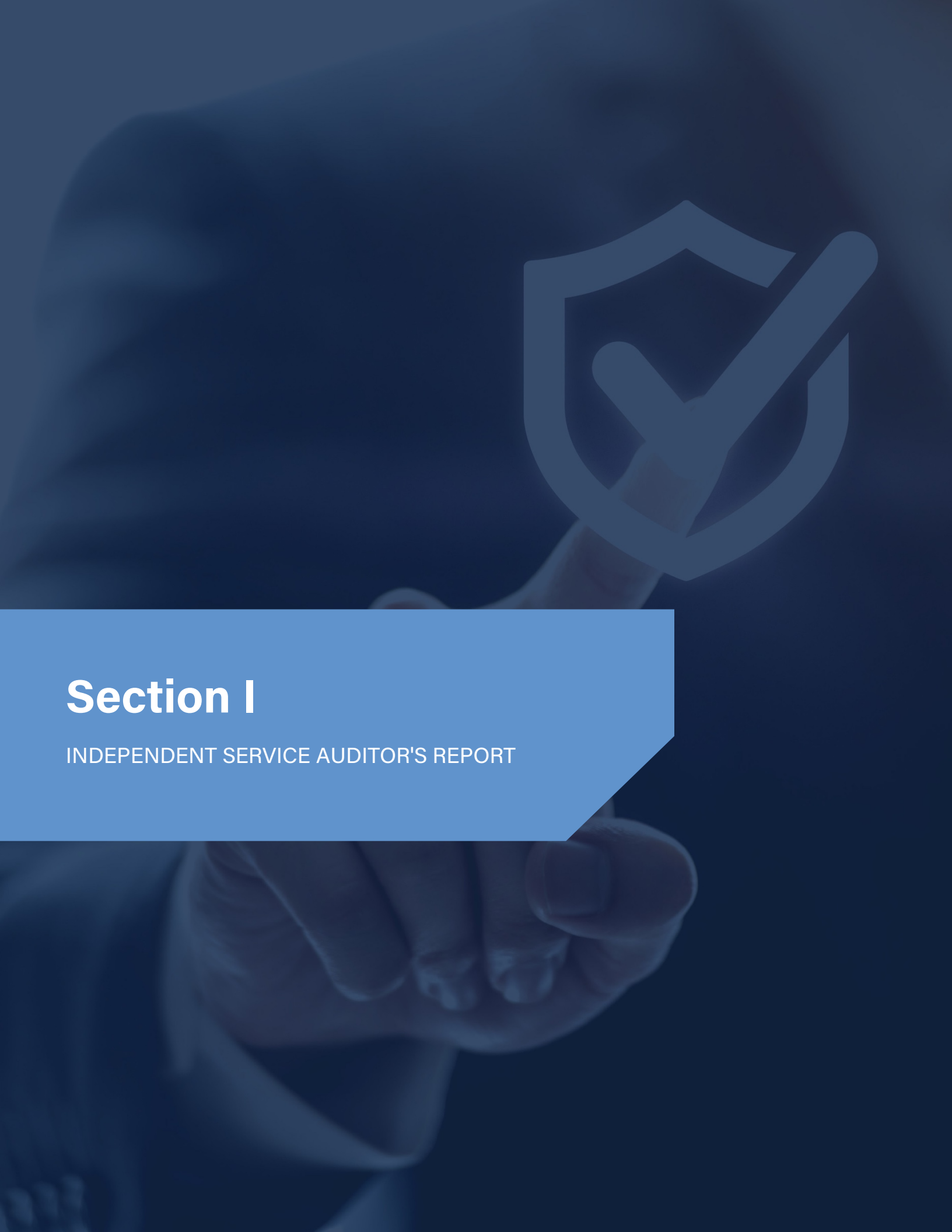
Together with Independent Service Auditor's Report

Report on Management's Description of

DevSamurai

TABLE OF CONTENTS





Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

DevSamurai, Inc.

Scope

We have examined DevSamurai, Inc.'s accompanying description of its Atlassian Marketplace Apps (system) titled "Description of Atlassian Marketplace Apps" throughout the period June 19, 2023 to September 19, 2023 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria),* (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 19, 2023 to September 19, 2023, to provide reasonable assurance that DevSamurai, Inc.'s service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

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

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

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

Service Auditor's Responsibilities

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls 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 and 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 Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a. The description presents DevSamurai, Inc.'s Atlassian Marketplace Apps (system) that was designed and implemented throughout the period June 19, 2023 to September 19, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period June 19, 2023 to September 19, 2023, to provide reasonable assurance that DevSamurai, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of DevSamurai, Inc.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period June 19, 2023 to September 19, 2023, to provide reasonable assurance that DevSamurai, Inc.'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 DevSamurai, Inc.'s controls operated effectively throughout the period.

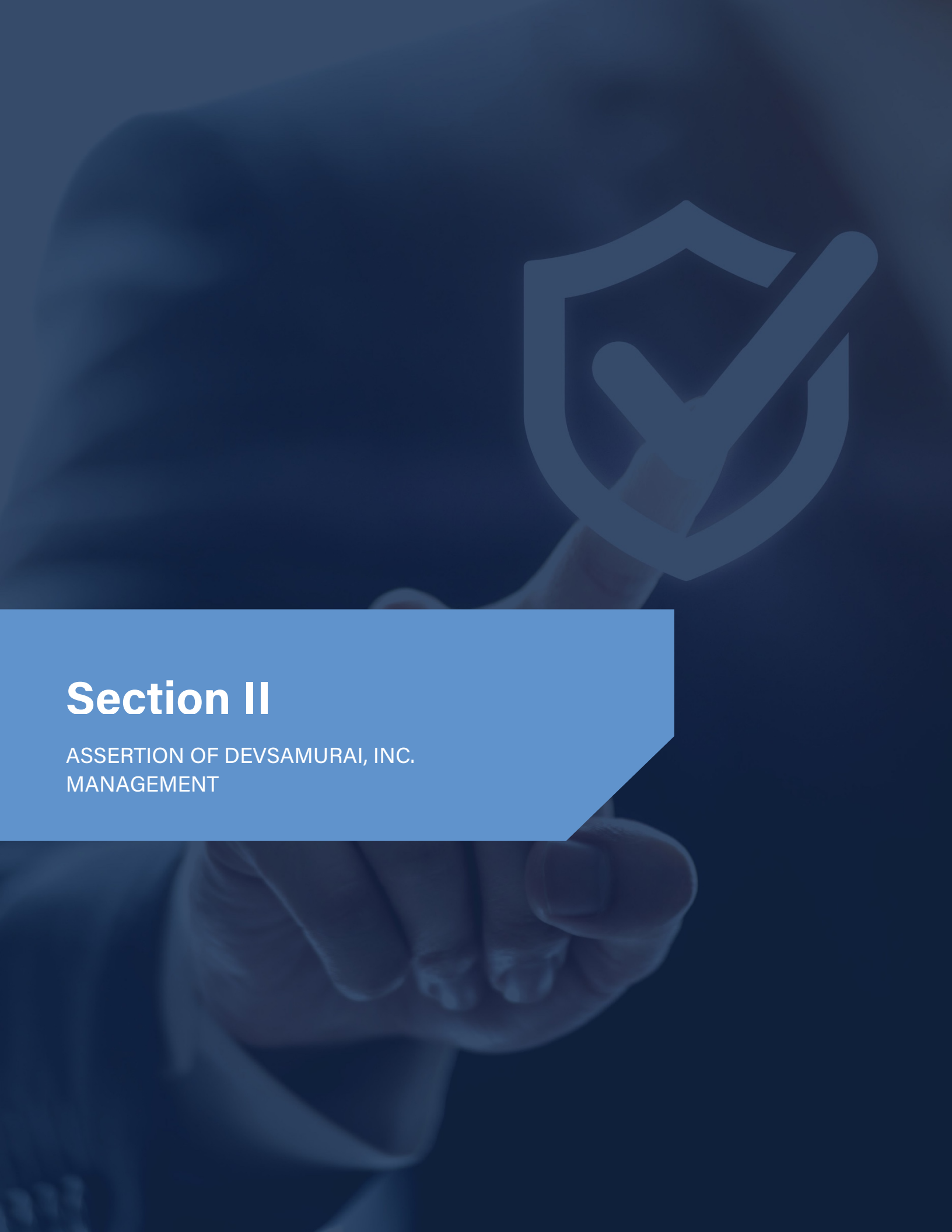
Restricted Use

This report, including the description of tests of controls and results thereof in the section of our report titled "Description of Test of Controls and Results Thereof" is intended solely for the information and use of DevSamurai, Inc.; user entities of DevSamurai, Inc.'s Atlassian Marketplace Apps during some or all of the period June 19, 2023 to September 19, 2023, business partners of DevSamurai, Inc. subject to risks arising from interactions with the DevSamurai, Inc.'s processing 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, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

JohansonGroup LLP
Colorado Springs, Colorado
November 11, 2023



Section II

ASSERTION OF DEVSAMURAI, INC.
MANAGEMENT

We have prepared the accompanying description of DevSamurai, Inc.'s "Description of Atlassian Marketplace Apps" for the period June 19, 2023 to September 19, 2023, (description) based on the criteria for a description of a service organization's system in DC section 200*, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)* (description criteria). The description is intended to provide report users with information about DevSamurai, Inc.'s Atlassian Marketplace Apps (system) that may be useful when assessing the risks arising from interactions with DevSamurai, Inc.'s system, particularly information about system controls that DevSamurai, Inc. 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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA, Trust Services Criteria).*

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

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

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

a. The description presents DevSamurai, Inc.'s Atlassian Marketplace Apps (system) that were designed and implemented throughout the period June 19, 2023 to September 19, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period June 19, 2023 to September 19, 2023, to provide reasonable assurance that DevSamurai, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of DevSamurai, Inc.'s controls throughout that period.
c. The controls stated in the description operated effectively throughout the period June 19, 2023 to September 19, 2023, to provide reasonable assurance that DevSamurai, Inc.'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 DevSamurai, Inc.'s controls operated effectively throughout that period.

DevSamurai, Inc. Management
November 11, 2023

Section III

DESCRIPTION OF ATLASSIAN MARKETPLACE APPS

COMPANY BACKGROUND

DevSamurai, Inc. ("DevSamurai" or "the Company") was founded on 17 October 2018 by Shin Nagasada to provide software and development services. The organization is based out of Tokyo, Japan

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

DevSamurai's core product, Atlassian marketplace apps (the "system") is a Software as a Service (SaaS) solution that includes the following services:

- Extend Atlassian Jira
- Project Management
- Agile Development tools

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

DevSamurai designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that DevSamurai makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that DevSamurai has established for the services. The system services are subject to the Security, Confidentiality, Availability, Processing Integrity, and/or Privacy commitments established internally for its services. Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems

COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:

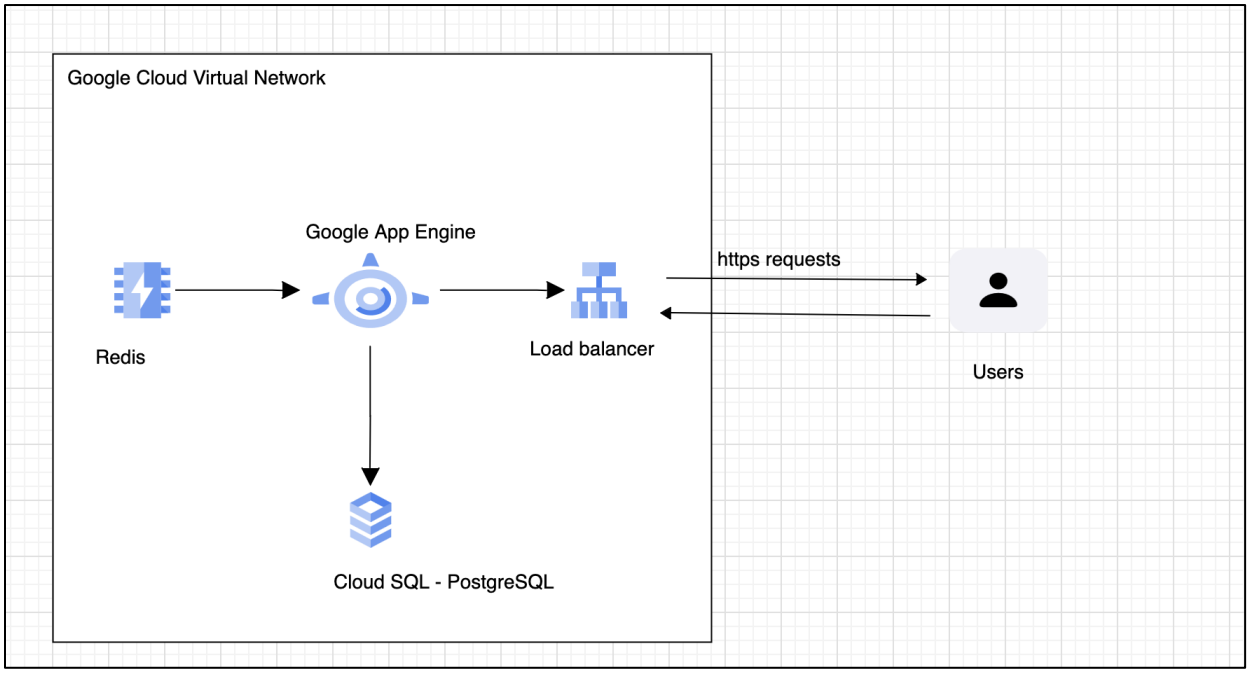
- *Infrastructure* – The collection of physical or virtual resources that support an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.

- *Software* - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.

- *People* - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- *Data* – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- *Procedures* – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

DevSamurai maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).



Primary Infrastructure		
Hardware	**Type**	**Purpose**
GCP Compute	Cloud Hosting Services	Virtual Private Cloud (VPC) environment that protects the network from unauthorized external access.
GCP Storage	Files storage	Store files and attachments
SQL Service	Database	Store data

Software

DevSamurai is responsible for managing the development and operation of the Jira app platform including infrastructure components such as servers, databases, and storage systems. The in-scope DevSamurai infrastructure and software components are shown in the table below:

Primary Software		
System/Application	**Operating System**	**Purpose**
Bitbucket	Codebase	Store code
Jira	Communication Service	

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

DevSamurai has a staff of approximately 2 organized in the following functional areas:

Management - Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

- CEO - Chief Executive Officer

Operations - Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology - Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development - Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data as defined by DevSamurai, constitutes the following:

- Company details and content created by DevSamurai
- Data generated in the company's apps

Data is categorized into four major types of data used by DevSamurai:

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for DevSamurai.	▪ Press releases ▪ Public website
Internal	Access to internal information is approved by management and is protected from external access.	▪ Internal memos ▪ Design documents ▪ Product specifications ▪ Correspondences
Customer data	Information received from customers for processing or storage by DevSamurai. DevSamurai must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	▪ Customer operating data ▪ App settings ▪ App data
Company data	Information collected and used by DevSamurai to operate the business. DevSamurai must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	▪ Legal documents ▪ Contractual agreements ▪ Employee PII ▪ Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, protect customer data. Additionally, DevSamurai has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by Shin Nagasada. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

DevSamurai's production servers are maintained by Google Cloud. The physical and environmental security protections are the responsibility of Google Cloud. DevSamurai reviews the attestation reports and performs a risk analysis of Google Cloud on at least an annual basis.

Logical Access

DevSamurai provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into three levels: Administrator, User, and No Access. User access and roles are reviewed on a quarterly basis to ensure the least privileged access.

Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing DevSamurai's policies and completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in-scope systems within 30 days of that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the IT team for completion and exceptions. If there is an exception, the IT team performs troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in Google Cloud with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

DevSamurai maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

DevSamurai internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

DevSamurai utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

DevSamurai maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

DevSamurai has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the DevSamurai application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

DevSamurai engages an external security firm to perform quarterly vulnerability scans and annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

This report does not include the Cloud Hosting Services provided by GCP at multiple facilities.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage, and ii. 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.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

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 DevSamurai's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of DevSamurai's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

DevSamurai's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The DevSamurai management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way DevSamurai can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require DevSamurai to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

DevSamurai's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

DevSamurai's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring 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.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

DevSamurai's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. DevSamurai's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

DevSamurai's risk assessment process identifies and manages risks that could potentially affect DevSamurai's ability to provide reliable and secure services to our customers. As part of this process, DevSamurai maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular DevSamurai product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of DevSamurai's system; as well as the nature of the components of the system result in risks that the criteria will not be met. DevSamurai addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, DevSamurai's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are integral components of DevSamurai's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

DevSamurai uses several information and communication channels internally to share information with management, employees, contractors, and customers. DevSamurai uses chat systems and email as the primary internal and external communication channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, DevSamurai uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. DevSamurai's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going Monitoring

DevSamurai's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in DevSamurai's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of DevSamurai's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities during the review period or since the organization's last review.

INCIDENTS

No significant incidents have occurred to the services provided to user entities during the review period or since the organization's last review.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Criteria/Security criteria were applicable to the DevSamurai Atlassian marketplace apps system.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by GCP at multiple facilities.

Subservice Description of Services

The Cloud Hosting Services provided by GCP support the physical infrastructure of the entity's services.

Subservice Provider – GCP		
Category	**Criteria**	**Control**
Security	CC6.4	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanisms, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.

		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real-time video surveillance and/or alerts generated by security systems.

DevSamurai management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, DevSamurai performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

DevSamurai's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to DevSamurai's services to be solely achieved by DevSamurai control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of DevSamurai.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to DevSamurai.
2. User entities are responsible for notifying DevSamurai of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of DevSamurai services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize DevSamurai services.
6. User entities are responsible for providing DevSamurai with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying DevSamurai of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Section IV

DESCRIPTION OF TEST OF CONTROLS AND RESULTS THEREOF

Relevant trust services criteria and DevSamurai, Inc.-related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if DevSamurai, Inc.'s controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* throughout the period June 19, 2023 to September 19, 2023.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of DevSamurai, Inc. activities and operations, and inspection of DevSamurai, Inc. documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all DevSamurai, Inc. controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria for the Security Category	***Description of DevSamurai, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
Control Environment			
CC 1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No events to test.
	The company performs background checks on new employees.	Inspected a sample of new hires for whom a background check is required to determine that they have a background check on file.	No events to test.
	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the company's example contractor agreement to determine that it includes a code of conduct or reference to the company code of conduct.	No exceptions noted.
	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected documentation to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the company's Code of Conduct to determine that it was in place, accessible to all employees, and that all employees must accept it upon hire.	No exceptions noted.
	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected documentation to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No events to test.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected documentation to determine that the company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	No exceptions noted.
	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's board of directors charter or policy to determine that it outlines its oversight responsibilities for internal control.	No exceptions noted.
	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the most recent board of directors meeting minutes and agenda to determine that the company's board of directors meets at least annually.	No exceptions noted.
	The company's Board of Directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the most recent Board of Directors meeting minutes and agenda to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The meeting minutes include feedback and direction from the board to the management as needed.	No exceptions noted.
CC 1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the most recent company organization chart to determine that it describes the organizational structure and reporting lines.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's security policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's board of directors charter or policy to determine that it outlines its oversight responsibilities for internal control.	No exceptions noted.
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No events to test.
	The company performs background checks on new employees.	Inspected all employees for whom a background check is required to determine that they have a background check on file.	No events to test.
	The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Inspected documentation to determine that the company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	No exceptions noted.
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No events to test.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the company's Code of Conduct to determine that it was in place, accessible to all employees, and that all employees must accept it upon hire.	No exceptions noted.
Communication and Information			
CC 2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the infrastructure configuration to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC 2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company communicates system changes to authorized internal users.	Inspected the internal communication to determine that the company communicates system changes to authorized internal users.	No events to test.
	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected documentation to determine that the company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's security policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company provides a description of its products and services to internal and external users.	Inspected documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Inspected documentation to determine that the company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No events to test.
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company website to determine that the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
	The company notifies customers of critical system changes that may affect their processing.	Inspected the company website to determine that they notify customers of critical system changes that may affect their processing.	No events to test.
	The company provides a description of its products and services to internal and external users.	Inspected documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company website to determine that they provide guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected documentation to determine that the company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Risk Assessment			
CC 3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected documentation to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No events to test.
CC 3.2 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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No events to test.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No events to test.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No events to test.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's configuration management procedure to determine that it was in place and ensured that system configurations were deployed consistently throughout the environment.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No events to test.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No events to test.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Monitoring Activities			
CC 4.1 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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No events to test.
CC 4.2 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.	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
Control Activities			
CC 5.1 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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No events to test.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No events to test.
CC 5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected documentation to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No events to test.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's data backup policy documents requirements for the backup and recovery of customer data.	Inspected the data backup policy to determine that it documents requirements for backup and recovery of customer data.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No events to test.
Logical and Physical Access			
CC 6.1 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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No events to test.
	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's data classification policy to determine that it ensures that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
	The company maintains a formal inventory of production system assets.	Inspected documentation to determine that the company maintains a formal inventory of production system assets.	No exceptions noted.
	The company requires authentication to systems and applications to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to systems and applications to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the company's passwords for in-scope system components to determine that it is configured according to the company's policy.	No exceptions noted.
	The company restricts access to migrate changes to production to authorized personnel.	Inspected access to migrate changes to production to determine that the company restricts privileged access to authorized personnel.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company restricts privileged access to databases to authorized users with a business need.	Inspected access to databases to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to encryption keys to authorized users with a business need.	Not Applicable - Control is implemented and maintained by subservice organizations.	No exceptions noted.
	The company restricts privileged access to the application to authorized users with a business need.	Inspected access to the application to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the firewall configuration to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the production network to authorized users with a business need.	Inspected access to the production network to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company's data stores housing sensitive customer data are encrypted at rest.	Inspected the company's data stores housing sensitive customer data to determine that they are encrypted at rest.	No exceptions noted.
	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the company's network configuration to determine that it is segmented to prevent unauthorized access to customer data.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 6.2 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No events to test.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
CC 6.3 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No events to test.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documents requirements for adding, modifying, and removing user access.	No exceptions noted.
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company requires visitors to sign in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	Inspected documentation to determine that the company requires visitors to sign in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	No exceptions noted.
	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Not Applicable - Control is implemented and maintained by subservice organizations.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 6.5 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the company's Asset Management Policy to determine that it provides guidance for proper asset disposal. Electronic media containing confidential information is purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	No events to test.
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected documentation to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No events to test.
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the firewall rulesets to determine that it is reviewed at least annually. Required changes are tracked to completion.	No events to test.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the company's firewall configuration to determine that they prevent unauthorized access.	No exceptions noted.
	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's secure data transmission protocols to determine that they encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's network and system hardening standards to determine that they are reviewed at least annually based on industry best practices.	No events to test.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's production systems to determine that it can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC 6.7 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.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the company's mobile device management (MDM) system to determine that it is in place to centrally manage mobile devices supporting the service.	No exceptions noted.
	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's secure data transmission protocols to determine that they encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the company's anti-malware technology to determine that it is configured to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
System Operations			
CC 7.1 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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's configuration management procedure to determine that it was in place and ensured that system configurations were deployed consistently throughout the environment.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Inspected the company's formal policies to determine that they outline the requirements for IT-related functions such as vulnerability management and system monitoring.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No events to test.
CC 7.2 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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the infrastructure monitoring tool to determine that it is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the infrastructure configuration to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Inspected the company's formal policies to determine that they outline the requirements for IT-related functions such as vulnerability management and system monitoring.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No events to test.
CC 7.3 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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected the company's incident response plan to determine that it is tested at least annually.	No events to test.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No events to test.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected the company's incident response plan to determine that it is tested at least annually.	No events to test.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Change Management			
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company restricts access to migrate changes to production to authorized personnel.	Inspected access to migrate changes to production to determine that the company restricts privileged access to authorized personnel.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's network and system hardening standards to determine that they are reviewed at least annually based on industry best practices.	No events to test.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No events to test.

Trust Services Criteria for the Security Category	*Description of DevSamurai, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plans to determine that they outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No events to test.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.