StateSet

System and Organization Controls (SOC) 2 Type 1

Report on Stateset Inc.'s Description of Its Autonomous Commerce Operations Platform and the Suitability of the Design of Its Controls Relevant to Security

As of November 21, 2024

Modern Assurance

The report accompanying this description was issued by Modern Assurance, LLC.

Table of Contents

Section I: Independent Service Auditor’s Report

Independent Service Auditor's Report

To the Management of Stateset Inc.,

Scope

We have examined Stateset Inc.'s (StateSet's) accompanying description of its autonomous commerce operations platform (system) titled, "Stateset Inc.'s Description of Its Autonomous Commerce Operations Platform" as of November 21, 2024 (description) based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design of controls stated in the description as of November 21, 2024, to provide reasonable assurance that StateSet's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Criteria*).

StateSet uses the subservice organizations described in the "Subservice Organizations" subsection of Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at StateSet, to achieve StateSet's service commitments and system requirements based on the applicable trust services criteria. The description presents StateSet's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of StateSet's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

StateSet 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 StateSet's service commitments and system requirements were achieved. StateSet has provided the accompanying assertion titled, "Stateset Inc.'s Management Assertion" (assertion), about the description and the suitability of design of controls described therein. StateSet is also responsible for preparing the description and assertion, including the completeness, accuracy, and

method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design 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 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- 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.
- evaluating the overall presentation of the description.

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

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

Inherent Limitations

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

important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects—

- The description presents StateSet's autonomous commerce operations platform that was designed and implemented as of November 21, 2024, in accordance with the description criteria.
- The controls stated in the description were suitably designed as of November 21, 2024, to provide reasonable assurance that StateSet's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of StateSet's controls as of that date.

Restricted Use

This report is intended solely for the information and use of StateSet, user entities of StateSet's autonomous commerce operations platform as of November 21, 2024, business partners of StateSet subject to risks arising from interactions with the autonomous commerce operations platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary 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.

Modern Assurance, LLC

November 21, 2024
Bend, Oregon

Section II: Stateset Inc.'s Management Assertion

Stateset Inc.'s Management Assertion

We have prepared the accompanying description of Stateset Inc.'s (StateSet's, service organization's) autonomous commerce operations platform titled "Stateset Inc.'s Description of Its Autonomous Commerce Operations Platform" as of November 21, 2024(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 users with information about the autonomous commerce operations platform that may be useful when assessing the risks arising from interactions with StateSet's system, particularly information about system controls that StateSet 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)*.

StateSet uses the subservice organizations described in the "Subservice Organizations" subsection of Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at StateSet, to achieve StateSet's service commitments and system requirements based on the applicable trust services criteria. The description presents StateSet's controls; the applicable trust services criteria; and the types of complementary subservice organization controls assumed in the design of StateSet's controls. The description does not disclose the actual controls at any subservice organization.

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

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

- The description presents StateSet's autonomous commerce operations platform that was designed and implemented as of November 21, 2024, in accordance with the description criteria.

- The controls stated in the description were suitably designed as of November 21, 2024, to provide reasonable assurance that StateSet's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively as of that date and if user entities and the subservice organizations applied the complementary controls assumed in the design of StateSet's controls as of that date.

Section III: Stateset Inc.'s Description of Its Autonomous Commerce Operations Platform

Stateset Inc.'s Description of Its Autonomous Commerce Operations Platform

Overview of the Company and Types of Services Provided

Stateset Inc. (“StateSet” or “the Company”) is a software as a service (SaaS) company building the next generation of commerce operations software, powered by AI and automation. Stateset is not just improving existing systems; it is redefining what's possible in the global commerce landscape. Its mission is to empower fast-growing direct-to-consumer brands with an autonomous commerce operating system that eliminates operational friction, enhances customer experiences, and drives unprecedented growth.

The scope of this report includes the autonomous commerce operations platform.

Principal Service Commitments and System Requirements

StateSet and its customers have a shared responsibility in maintaining the security of the autonomous commerce operations platform. StateSet has established principal service commitments, which are communicated via service agreements and consist of the following:

- Defines and documents roles and responsibilities related to the Company’s Information Security Program and the protection of customer data. Requires team members to review and accept all of the security policies.
- Requires team members to go through employee security awareness training covering industry standard practices and information security topics such as phishing and password management.
- Follows the principle of least privilege with respect to identity and access management.
- Maintains administrative, physical, and technical safeguards
  for protection of the security, confidentiality and integrity of data.
- Encrypts data in transit using transport layer security (TLS) or other technologies over public networks.
- Performs an independent third-party penetration at least annually to ensure that the security posture of services is uncompromised.
- Actively monitors and logs various cloud services.

StateSet has established system requirements, which are communicated via service agreements and consist of the following:

- Employee provisioning and deprovisioning standards
- User access reviews

- Logical access controls, such as the use of user IDs and passwords to access systems
- Encryption standards for data at rest and in transit
- Business continuity and disaster recovery plan

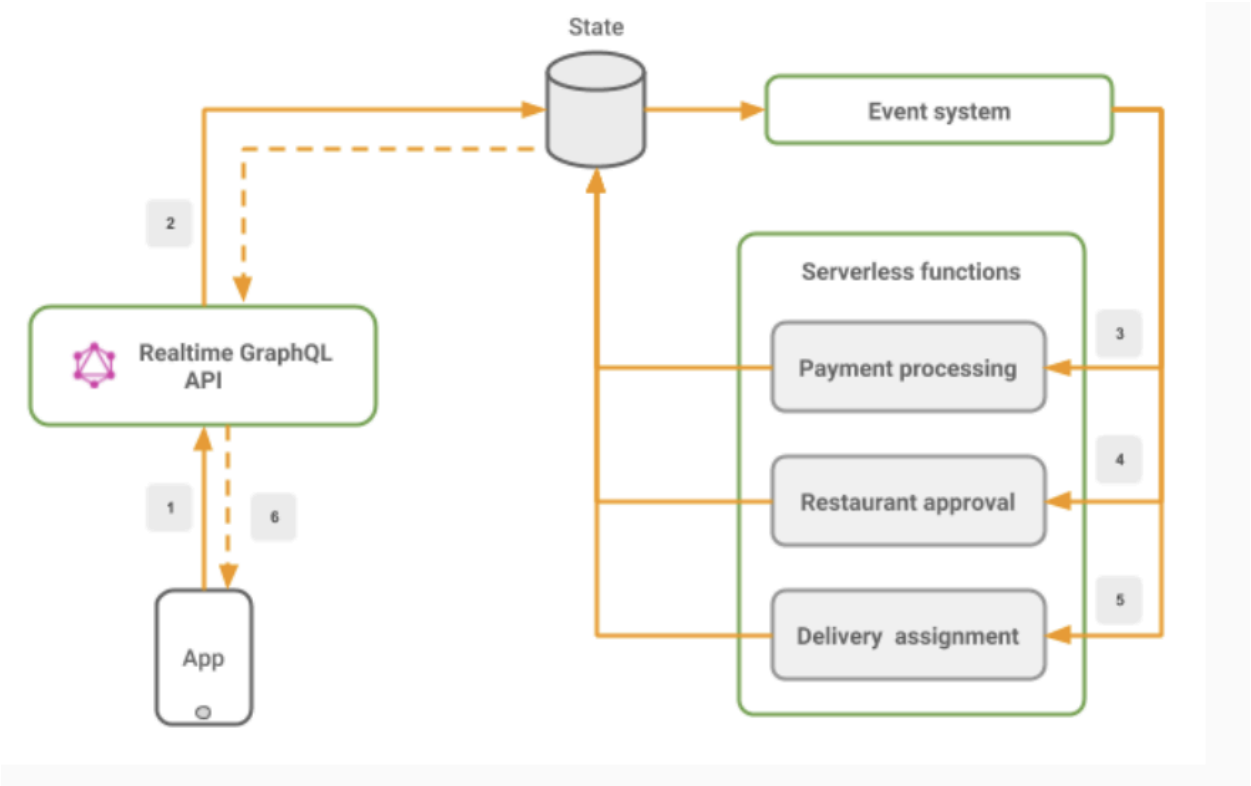
Components of the System

Infrastructure

The Autonomous Commerce Operations Platform is comprised of the following components:

Component	Description	Cloud Provider
Stateset One Web App	Front end platform for clients for customer orchestration	Vercel
Hasura API	GraphQL API's that communicate with the Stateset Cloud Platform	GCP
Temporal API	Deterministic Workflow Queue and Scheduler that communicate with the StateSet Cloud Platform	GCP
Hasura API- Legacy	GraphQL API's that communicate with the Stateset Cloud Platform- for legacy clients	Heroku
Stateset Cloud Platform	Internally used web application for Stateset's view into the workflow infrastructure	GCP
RestAPI	API's that ingest data from third party integrations (commerce sites)	GCP

The platform’s components operate according to the following architecture diagram:



Software

StateSet utilizes the following software to support the platform:

Function	Software used
Authentication manager	GoogleWorkspace, Clerk
Human resources	Rippling
Password management	1Password
Ticketing	Linear
Change management and deployment	Gitlab, ArgoCD, Vercel tools
Monitoring and logging	GCP security monitoring, Vercel security monitoring, Logflare

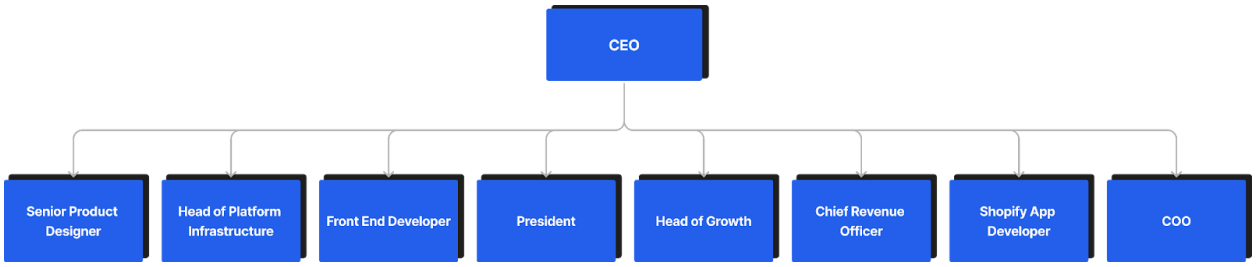
Data

Data is classified in accordance with the written Data Classification Policy. Data is ingested into the Stateset Cloud Platform through customer input into the Web App or through API integrations with third parties. Data is stored in PostgreSQL on Heroku and in PostgreSQL on GCP. The databases housing sensitive customer data are encrypted at rest by the vendors. Sensitive data is not transmitted outside of StateSet's environment. The Company uses HTTPS to encrypt confidential and sensitive data when transmitted over public networks **(AC-11)**. All in-scope cloud resources containing either customer data or production infrastructure are restricted to not allow public access without first authenticating **(AC-13)**.

People

StateSet's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

StateSet has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting. The organizational chart can be referenced below:



Policies

StateSet has implemented the following policies, which serve as the basis for Company procedures, are made accessible to all relevant employees and contractors, and are reviewed annually:

- Acceptable Use Policy - defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access. This policy is acknowledged by new hire employees and contractors upon hire **(ORG-10).**
- Access Control and Termination Policy - governs authentication and access to applications, resources, and tools **(AC-04).**
- Business Continuity and Disaster Recovery Policy - governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption **(AVA-04).**

- Change Management Policy - governs the documentation, tracking, testing, and approving of system, network, security, and infrastructure changes for applications, resources, and tools **(CM-07).**
- Code of Conduct - outlines ethical expectations, behavior standards, and ramifications of non compliance. This policy is acknowledged by new hire employees and contractors upon hire **(ORG-01).**
- Configuration and Asset Management Policy - governs configurations for new applications, resources, and tools **(CM-06).**
- Encryption and Key Management Policy - supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls **(AC-12).**
- Information Security Policy - establishes the security requirements for maintaining the security of applications, resources, and tools **(ORG-12).**
- Internal Control Policy - identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies **(ORG-14).**
- Network Security Policy - identifies the requirements for protecting information and systems within and across networks **(NET-06).**
- Performance Review Policy - provides personnel context and transparency into their performance and career development processes **(ORG-15).**
- Risk Assessment and Treatment Policy - governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners **(RA-01).**
- Secure Development Policy - defines the requirements for secure software and system development and maintenance **(CM-08).**
- Security Incident Response Plan - outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution **(IR-01).**
- Vendor Management Policy - defines a framework for the onboarding and management of the vendor relationship cycle **(RA-04).**
- Vulnerability Management and Patch Management Policy - outlines the processes to identify and respond to vulnerabilities **(VM-01).**

Applicable Trust Services Criteria and the Related Controls

Control Environment

The objectives of internal control as it relates to the autonomous commerce operations platform are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant control objectives, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of StateSet employees, the policies and procedures, the risk management process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on StateSet's assessment of risk facing the organization.

Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of StateSet's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and Code of Conduct, and by the examples the executives set. StateSet's executive management recognizes their responsibility to foster a strong ethical environment within StateSet to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Code of Conduct, which is distributed to all applicable personnel of the organization.

Governance and Structure

Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters **(ORG-03).** Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel through Rippling **(ORG-06).** Additionally, roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and in the Information Security Policy **(ORG-18).**

New Personnel

The Company is committed to maintaining a strong culture of professionalism and exemplary behavior. As a foundation to ensure consistency in culture across the organization, the Company has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. New hires are required to acknowledge acceptance and adherence to the Code of Conduct upon hiring **(ORG-01).** Background checks are completed for

new employees and contractors shortly after hiring as permitted by local laws **(ORG-07).** To help maintain a high level of performance among staff members within the organization, hiring managers screen new hires to assess their qualifications, experience, and competency to fulfill their responsibilities **(ORG-08).**

Additionally, all relevant internal personnel with system access are required to complete training programs upon hire and annually thereafter related to information security to help them understand their obligations and responsibilities related to security **(ORG-09).** The company's policies clearly document that personnel who violate information security policies are subject to disciplinary action commensurate with the violation **(ORG-11).**

Risk Assessment Process

StateSet has defined a risk management framework for evaluating information security risk and other relevant forms of business risk. A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud **(RA-02).** A risk register is maintained to record the risk mitigation strategies for identified risks, and to track the development or modification of controls consistent with the risk mitigation strategy **(RA-03).**

Due to the company's heavy reliance on outside vendors for critical infrastructure, processing capabilities, and business functions, the company has developed a Vendor Management Policy which establishes the compliance and performance expectations required of vendors, and the due diligence and monitoring expectations required of the Company's personnel. Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy **(RA-06).** StateSet collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis **(RA-05).**

Information and Communication

Information and communication is an integral component of StateSet'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. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At StateSet, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

As part of the Company's commitment to communication, it provides descriptions of its services and systems on its website, which is available to both internal personnel and external users **(COM-01).** The company's commitments with respect to security are published on the company's website **(COM-03).**

In order to enable communication channels from both internal and external sources, StateSet provides an email on its public website so that both internal personnel and external users can

report security concerns. Management monitors communications from the channel and responds in accordance with the Security Incident Response Plan **(COM-05).** The Change Management Policy and Security Incident Response Plan detail the requirements for communication to external parties following a system change, an incident, or unauthorized disclosure of sensitive information **(COM-04).**

Monitoring Activities

StateSet performs several types of monitoring to assess the security of health of the in-scope environment and the related controls. The company leverages a continuous monitoring solution that monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve **(ORG-05).**

Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable **(NET-04).** Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution **(NET-05).** The Security Steering Committee meets quarterly to coordinate security initiatives and review network security, management of infrastructure and discuss security risks **(NET-07)**.

Control Activities

Access Control

Users are provisioned new or modified access to the in-scope systems (Stateset Web App, Cloud Platform, Vercel, GCP, Heroku, Clerk, ArgoCD, Google Workspace, Gitlab, Rippling) based on the established Onboarding Policy document or a documented business reason and approval by the system owner or manager **(AC-07).** These systems are configured to require users to establish strong, complex passwords and, for all in-scope systems a second form of authentication is required **(AC-03).** To maintain accountability and password security, personnel are assigned unique IDs to access in-scope applications, data, resources, and tools, and shared accounts are not used **(AC-02).**

Upon employee or contractor termination, access to in-scope applications, resources, and tools is removed within 24 hours of last day **(AC-08).** The CEO reviews quarterly reviews of user access to the in-scope systems in accordance with policy documentation requirements to validate that user access remains commensurate with job responsibilities. Access identified during the review as requiring revocation is completed within a timely manner **(AC-09).**

Change Management

The Company uses Gitlab as a secure code repository, which is configured to manage changes to the codebases for the autonomous commerce operations platform to help ensure version control for secure deployment to the production environment **(CM-01).** Separate environments are used

in the change management cycle to develop, test, and stage changes prior to deployment into production **(CM-04).** Code changes are tested using automated testing scripts prior to being merged to the production branch **(CM-02).** Access to the code repository is limited to appropriate individuals and all code changes require a merge request **(CM-03)**. Notifications are sent to personnel when changes are deployed into production **(CM-09).**

Configuration and Vulnerability Management

To help ensure that key configurations related to networking ports, protocols, and services, and firewalls were initially configured to appropriately restrict outside traffic and that they remain appropriately restricted over time, StateSet performs a review annually of its key network configurations. The configurations that are identified during the review as needing to be changed are tracked to resolution **(NET-03).** Vulnerability scanning is performed continuously on infrastructure using GKE Security, and identified high and critical vulnerabilities are remediated as soon as possible **(VM-02).** A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution **(VM-03).**

Incident Response and Business Continuity

The Company employs multiple mechanisms to identify potential security incidents as discussed in the *Communication* and *Monitoring* sections above. Confirmed incidents are documented, tracked, and responded to according to the Security Incident Response Plan **(IR-02).** Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes **(IR-03).** The Security Incident Response Plan is tested at least annually to assess effectiveness, and management makes changes to the Security Incident Response Plan based on the test results **(IR-04).**

Complementary User Entity Controls

The following user entity controls are assumed to be implemented by user entities and are necessary for the service organization's service commitments and system requirements to be achieved.

User Entity Control	Relevant Criteria
User entities are responsible for setting up, monitoring, and removing user entity access to the system and ensuring that it is appropriate.	CC 6.1, CC 6.2, CC 6.3, CC 6.6
User entities are responsible for understanding and complying with their contractual obligations to StateSet.	CC 2.2, CC 2.3

User Entity Control	Relevant Criteria
User entities are responsible for immediately notifying StateSet of any actual or suspected information security breaches, including compromised user accounts.	CC 2.2
User entities are responsible for ensuring the supervision, management, and control of the use of StateSet's services by their personnel.	CC 4.2
User entities are responsible for ensuring that only authorized and properly trained personnel are allowed access to the services.	CC 5.3

Subservice Organizations

The Company utilizes the subservice organizations in the below tables to achieve its objectives.

Additionally, the Company has implemented the following control to monitor the services provided by the subservice organizations: *The SOC 2 reports (or security due diligence equivalent) of StateSet's high risk vendors are collected and reviewed on at least an annual basis* ***(RA-05).***

Subservice Organization	Services Provided
Google LLC (Google Cloud Platform)	The subservice organization provides the Company with cloud infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized

Subservice Organization	Services Provided
Google LLC (Google Cloud Platform)	The subservice organization provides the Company with cloud infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).

- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Subservice Organization	Services Provided
Salesforce, Inc. (Heroku)	The subservice organization provides the Company with cloud-based platform services. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to

Subservice Organization	Services Provided
Salesforce, Inc. (Heroku)	The subservice organization provides the Company with cloud-based platform services. This organization was carved out of the report.

Complementary Subservice Organization Controls

ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).

- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Subservice Organization	Services Provided
Vercel Inc.	The subservice organization provides the Company with front-end hosting services. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Subservice Organization	Services Provided
Gitlab B.V.	The subservice organization provides the Company with cloud-based source control software. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Section IV: Stateset Inc.'s Controls

Stateset Inc.'s Controls

Within the following table, the security criteria and the related control activities have been specified by, and are the responsibility of, StateSet.

CC1.0 COMMON CRITERIA RELATED TO CONTROL ENVIRONMENT	
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
ORG-01	The Company has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. New hires are required to acknowledge acceptance and adherence to the Code of Conduct upon hiring.
ORG-11	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.

CC1.0 COMMON CRITERIA RELATED TO CONTROL ENVIRONMENT	
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.

CC1.0 COMMON CRITERIA RELATED TO CONTROL ENVIRONMENT	
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.
ORG-06	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.
ORG-18	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.
RA-05	StateSet collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis.

RA-06	Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.

CC1.0 COMMON CRITERIA RELATED TO CONTROL ENVIRONMENT	
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
ORG-01	The Company has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. New hires are required to acknowledge acceptance and adherence to the Code of Conduct upon hiring.
ORG-07	Background checks are completed for new employees and contractors as defined by the policy and as permitted by local laws.
ORG-08	Hiring managers screen new hires to assess their qualifications, experience, and competency to fulfill their responsibilities.
ORG-09	Internal personnel complete training programs upon hire and annually thereafter according to the policy related to information security to help them understand their obligations and responsibilities related to security.
ORG-12	An Information Security Policy that establishes the security requirements for maintaining the security of applications, resources, and tools is accessible to all relevant employees and contractors, and is reviewed annually.
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.
ORG-15	A Performance Review Policy that provides personnel context and transparency into their performance and career development processes is accessible to all relevant employees, and is reviewed annually.
RA-05	StateSet collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis.

CC1.0 COMMON CRITERIA RELATED TO CONTROL ENVIRONMENT	
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.

ORG-05	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve.
ORG-06	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.
ORG-11	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.
ORG-15	A Performance Review Policy that provides personnel context and transparency into their performance and career development processes is accessible to all relevant employees, and is reviewed annually.

CC2.0 COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION	
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
COM-01	Descriptions of the company's services and systems are available to both internal personnel and external users.
NET-07	A Security Steering Committee meets quarterly to coordinate security initiatives and to review network security, management of infrastructure, and security risks.
ORG-05	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve.
ORG-12	An Information Security Policy that establishes the security requirements for maintaining the security of applications, resources, and tools is accessible to all relevant employees and contractors, and is reviewed annually.
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.
VM-02	Vulnerability scanning is performed on infrastructure systems, and identified deficiencies are remediated according to the policy.
VM-03	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.

CC2.0 COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION	
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
COM-01	Descriptions of the company's services and systems are available to both internal personnel and external users.
COM-05	Stateset has a reporting channel available to internal personnel and external users to report security concerns. Management monitors communications from the channel and responds in accordance with the Security Incident Response Plan.
IR-01	A Security Incident Response Plan that outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution is accessible to all relevant employees and contractors and is reviewed annually.
NET-06	A Network Security Policy that identifies the requirements for protecting information and systems within and across networks is accessible to all relevant employees and contractors and is reviewed annually.
ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.
ORG-09	Internal personnel complete training programs upon hire and annually thereafter according to the policy related to information security to help them understand their obligations and responsibilities related to security.
ORG-18	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.

CC2.0 COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION	
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
COM-01	Descriptions of the company's services and systems are available to both internal personnel and external users.
COM-03	The company's commitments with respect to security are published on the company's website.
COM-04	StateSet's Change Management Policy and Security Incident Response Plan detail the requirements for communication to external parties following a system change, an incident, or unauthorized disclosure of sensitive information.
COM-05	Stateset has a reporting channel available to internal personnel and external users to report security concerns. Management monitors communications from the channel and responds in accordance with the Security Incident Response Plan.

ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.
RA-06	Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.

CC3.0 COMMON CRITERIA RELATED TO RISK ASSESSMENT	
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.
RA-01	A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.

CC3.0 COMMON CRITERIA RELATED TO RISK ASSESSMENT	
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
RA-01	A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.
RA-03	A risk register is maintained to record the risk mitigation strategies for unmitigated risks, and to track the development or modification of controls consistent with the risk mitigation strategy.
RA-04	A Vendor Management Policy that defines a framework for the onboarding and management of the vendor relationship cycle is accessible to all relevant employees and contractors, and is reviewed annually.

RA-06	Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.
VM-02	Vulnerability scanning is performed on infrastructure systems, and identified deficiencies are remediated according to the policy.

CC3.0 COMMON CRITERIA RELATED TO RISK ASSESSMENT	
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.

CC3.0 COMMON CRITERIA RELATED TO RISK ASSESSMENT	
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.
RA-06	Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.

CC4.0 COMMON CRITERIA RELATED TO MONITORING ACTIVITIES	
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
NET-07	A Security Steering Committee meets quarterly to coordinate security initiatives and to review network security, management of infrastructure, and security risks.
ORG-05	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve.
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.
VM-02	Vulnerability scanning is performed on infrastructure systems, and identified deficiencies are remediated according to the policy.

VM-03	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.

CC4.0 COMMON CRITERIA RELATED TO MONITORING ACTIVITIES	
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
NET-07	A Security Steering Committee meets quarterly to coordinate security initiatives and to review network security, management of infrastructure, and security risks.
ORG-03	Senior management meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.
ORG-05	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve.
VM-02	Vulnerability scanning is performed on infrastructure systems, and identified deficiencies are remediated according to the policy.
VM-03	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.

CC5.0 COMMON CRITERIA RELATED TO CONTROL ACTIVITIES	
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.
RA-03	A risk register is maintained to record the risk mitigation strategies for unmitigated risks, and to track the development or modification of controls consistent with the risk mitigation strategy.

CC5.0 COMMON CRITERIA RELATED TO CONTROL ACTIVITIES	
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CM-08	A Secure Development Policy that defines the requirements for secure software and system development and maintenance is accessible to relevant employees and contractors and is reviewed annually.
ORG-05	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve.
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.
ORG-18	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.

CC5.0 COMMON CRITERIA RELATED TO CONTROL ACTIVITIES	
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
AC-04	An Access Control and Termination Policy that governs authentication and access to applications, resources, and tools is accessible to all relevant employees and contractors and is reviewed annually.
AC-12	An Encryption and Key Management Policy that supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls, is accessible to all relevant employees and contractors and is reviewed annually.
CM-06	A Configuration and Asset Management Policy that governs configurations for new applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
CM-07	A Change Management Policy that governs the documentation, tracking, testing, and approving of system, network, security, and infrastructure changes for applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
CM-08	A Secure Development Policy that defines the requirements for secure software and system development and maintenance is accessible to relevant employees and contractors and is reviewed annually.

IR-01	A Security Incident Response Plan that outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution is accessible to all relevant employees and contractors and is reviewed annually.
NET-06	A Network Security Policy that identifies the requirements for protecting information and systems within and across networks is accessible to all relevant employees and contractors and is reviewed annually.
ORG-05	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve.
ORG-10	An Acceptable Use Policy that defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access is acknowledged by new hire employees and contractors upon hire according to the policy, is accessible to all employees and contractors, and is reviewed annually.
ORG-11	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.
ORG-12	An Information Security Policy that establishes the security requirements for maintaining the security of applications, resources, and tools is accessible to all relevant employees and contractors, and is reviewed annually.
ORG-14	An Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies is accessible to all relevant employees and contractors, and is reviewed annually.
ORG-15	A Performance Review Policy that provides personnel context and transparency into their performance and career development processes is accessible to all relevant employees, and is reviewed annually.
ORG-18	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.
RA-01	A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
RA-04	A Vendor Management Policy that defines a framework for the onboarding and management of the vendor relationship cycle is accessible to all relevant employees and contractors, and is reviewed annually.

VM-01	A Vulnerability Management and Patch Management Policy that outlines the processes to identify and respond to vulnerabilities is accessible to all relevant employees and contractors, and is reviewed annually.
AVA-04	A Business Continuity and Disaster Recovery Policy that governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption is accessible to all relevant employees and contractors, and is reviewed annually.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
AC-02	Personnel are assigned unique IDs to access in-scope applications, data, resources, and tools, and shared accounts are not used.
AC-03	Personnel are required to use strong, complex passwords and a second form of authentication to access in-scope applications, data, resources, and tools in accordance with the policy.
AC-04	An Access Control and Termination Policy that governs authentication and access to applications, resources, and tools is accessible to all relevant employees and contractors and is reviewed annually.
AC-12	An Encryption and Key Management Policy that supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls, is accessible to all relevant employees and contractors and is reviewed annually.
AC-13	Cloud resources are configured to restrict public access.
CM-04	Separate environments are used in the change management cycle to develop, test, and stage changes prior to deployment into production.
CM-06	A Configuration and Asset Management Policy that governs configurations for new applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
NET-03	StateSet's environment is configured to restrict outside traffic. StateSet performs an annual review of its key configurations related to networking ports, protocols, services, and firewalls according to the policy to help ensure that the environment is restricted from outside traffic as necessary. Configurations identified during the review as requiring changes are tracked to resolution.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
AC-04	An Access Control and Termination Policy that governs authentication and access to applications, resources, and tools is accessible to all relevant employees and contractors and is reviewed annually.
AC-07	Users are provisioned new or modified access to systems based on the established Onboarding Policy or based on a documented business reason and approval by the system owner.
AC-08	Upon employee or contractor termination, access to in-scope applications, resources, and tools is removed according to the policy.
AC-09	System owners conduct periodic reviews of user access to in-scope applications, resources, and tools in accordance with policy documentation to validate that user access remains commensurate with job responsibilities. Identified access revocations are completed within a timely manner.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
AC-04	An Access Control and Termination Policy that governs authentication and access to applications, resources, and tools is accessible to all relevant employees and contractors and is reviewed annually.
AC-07	Users are provisioned new or modified access to systems based on the established Onboarding Policy or based on a documented business reason and approval by the system owner.
AC-08	Upon employee or contractor termination, access to in-scope applications, resources, and tools is removed according to the policy.
AC-09	System owners conduct periodic reviews of user access to in-scope applications, resources, and tools in accordance with policy documentation to validate that user access remains commensurate with job responsibilities. Identified access revocations are completed within a timely manner.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
RA-05	StateSet collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CM-06	A Configuration and Asset Management Policy that governs configurations for new applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
RA-05	StateSet collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
AC-03	Personnel are required to use strong, complex passwords and a second form of authentication to access in-scope applications, data, resources, and tools in accordance with the policy.
AC-11	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
AC-12	An Encryption and Key Management Policy that supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls, is accessible to all relevant employees and contractors and is reviewed annually.
AC-13	Cloud resources are configured to restrict public access.
NET-03	StateSet's environment is configured to restrict outside traffic. StateSet performs an annual review of its key configurations related to networking ports, protocols, services, and firewalls according to the policy to help ensure that the environment is restricted from outside traffic as necessary. Configurations identified during the review as requiring changes are tracked to resolution.

NET-06	A Network Security Policy that identifies the requirements for protecting information and systems within and across networks is accessible to all relevant employees and contractors and is reviewed annually.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
AC-11	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
ORG-10	An Acceptable Use Policy that defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access is acknowledged by new hire employees and contractors upon hire according to the policy, is accessible to all employees and contractors, and is reviewed annually.

CC6.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CM-01	A code repository is configured to manage changes to the codebases for applications for secure deployment to the production environment.
CM-02	Code changes are tested prior to being merged to the production branch.
CM-03	Access to the code repository is limited to appropriate individuals and all code changes require a merge request.
CM-06	A Configuration and Asset Management Policy that governs configurations for new applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
CM-07	A Change Management Policy that governs the documentation, tracking, testing, and approving of system, network, security, and infrastructure changes for applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
CM-09	Notifications are sent to personnel when changes are deployed into production.
ORG-10	An Acceptable Use Policy that defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access is acknowledged by new hire employees and contractors upon hire according to the policy, is accessible to all employees and contractors, and is reviewed annually.

CC7.0 COMMON CRITERIA RELATED TO SYSTEM OPERATIONS	
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
CM-01	A code repository is configured to manage changes to the codebases for applications for secure deployment to the production environment.
CM-06	A Configuration and Asset Management Policy that governs configurations for new applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
NET-03	StateSet's environment is configured to restrict outside traffic. StateSet performs an annual review of its key configurations related to networking ports, protocols, services, and firewalls according to the policy to help ensure that the environment is restricted from outside traffic as necessary. Configurations identified during the review as requiring changes are tracked to resolution.
NET-04	Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable.
NET-05	Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution.
VM-01	A Vulnerability Management and Patch Management Policy that outlines the processes to identify and respond to vulnerabilities is accessible to all relevant employees and contractors, and is reviewed annually.
VM-02	Vulnerability scanning is performed on infrastructure systems, and identified deficiencies are remediated according to the policy.
VM-03	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.

CC7.0 COMMON CRITERIA RELATED TO SYSTEM OPERATIONS	
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
NET-03	StateSet's environment is configured to restrict outside traffic. StateSet performs an annual review of its key configurations related to networking ports, protocols, services, and firewalls according to the policy to help ensure that the environment is restricted from outside traffic as necessary. Configurations identified during the review as requiring changes are tracked to resolution.
NET-04	Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable.
NET-05	Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution.
NET-06	A Network Security Policy that identifies the requirements for protecting information and systems within and across networks is accessible to all relevant employees and contractors and is reviewed annually.

CC7.0 COMMON CRITERIA RELATED TO SYSTEM OPERATIONS	
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
IR-01	A Security Incident Response Plan that outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution is accessible to all relevant employees and contractors and is reviewed annually.
IR-02	Identified incidents are documented, tracked, and responded to according to the Security Incident Response Plan.

CC7.0 COMMON CRITERIA RELATED TO SYSTEM OPERATIONS	
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
AVA-04	A Business Continuity and Disaster Recovery Policy that governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption is accessible to all relevant employees and contractors, and is reviewed annually.
COM-04	StateSet's Change Management Policy and Security Incident Response Plan detail the requirements for communication to external parties following a system change, an incident, or unauthorized disclosure of sensitive information.
IR-01	A Security Incident Response Plan that outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution is accessible to all relevant employees and contractors and is reviewed annually.
IR-02	Identified incidents are documented, tracked, and responded to according to the Security Incident Response Plan.
IR-03	Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes.
IR-04	The Security Incident Response Plan is tested at least annually to assess effectiveness, and management makes changes to the Security Incident Response Plan based on the test results.
ORG-11	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.

CC7.0 COMMON CRITERIA RELATED TO SYSTEM OPERATIONS	
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	
COM-04	StateSet's Change Management Policy and Security Incident Response Plan detail the requirements for communication to external parties following a system change, an incident, or unauthorized disclosure of sensitive information.
IR-01	A Security Incident Response Plan that outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution is accessible to all relevant employees and contractors and is reviewed annually.
IR-02	Identified incidents are documented, tracked, and responded to according to the Security Incident Response Plan.

IR-03	Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes.
IR-04	The Security Incident Response Plan is tested at least annually to assess effectiveness, and management makes changes to the Security Incident Response Plan based on the test results.

CC8.0 COMMON CRITERIA RELATED TO CHANGE MANAGEMENT	
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CM-01	A code repository is configured to manage changes to the codebases for applications for secure deployment to the production environment.
CM-02	Code changes are tested prior to being merged to the production branch.
CM-03	Access to the code repository is limited to appropriate individuals and all code changes require a merge request.
CM-04	Separate environments are used in the change management cycle to develop, test, and stage changes prior to deployment into production.
CM-06	A Configuration and Asset Management Policy that governs configurations for new applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
CM-07	A Change Management Policy that governs the documentation, tracking, testing, and approving of system, network, security, and infrastructure changes for applications, resources, and tools is accessible to relevant employees and contractors and is reviewed annually.
CM-08	A Secure Development Policy that defines the requirements for secure software and system development and maintenance is accessible to relevant employees and contractors and is reviewed annually.
CM-09	Notifications are sent to personnel when changes are deployed into production.

CC9.0 COMMON CRITERIA RELATED TO RISK MITIGATION	
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
AVA-04	A Business Continuity and Disaster Recovery Policy that governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption is accessible to all relevant employees and contractors, and is reviewed annually.

IR-01	A Security Incident Response Plan that outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution is accessible to all relevant employees and contractors and is reviewed annually.
RA-01	A Risk Assessment and Treatment Policy that governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners is accessible to all relevant employees and contractors, and is reviewed annually.
RA-02	A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud.
RA-03	A risk register is maintained to record the risk mitigation strategies for unmitigated risks, and to track the development or modification of controls consistent with the risk mitigation strategy.

CC9.0 COMMON CRITERIA RELATED TO RISK MITIGATION	
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	
RA-04	A Vendor Management Policy that defines a framework for the onboarding and management of the vendor relationship cycle is accessible to all relevant employees and contractors, and is reviewed annually.
RA-05	StateSet collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis.
RA-06	Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy.