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

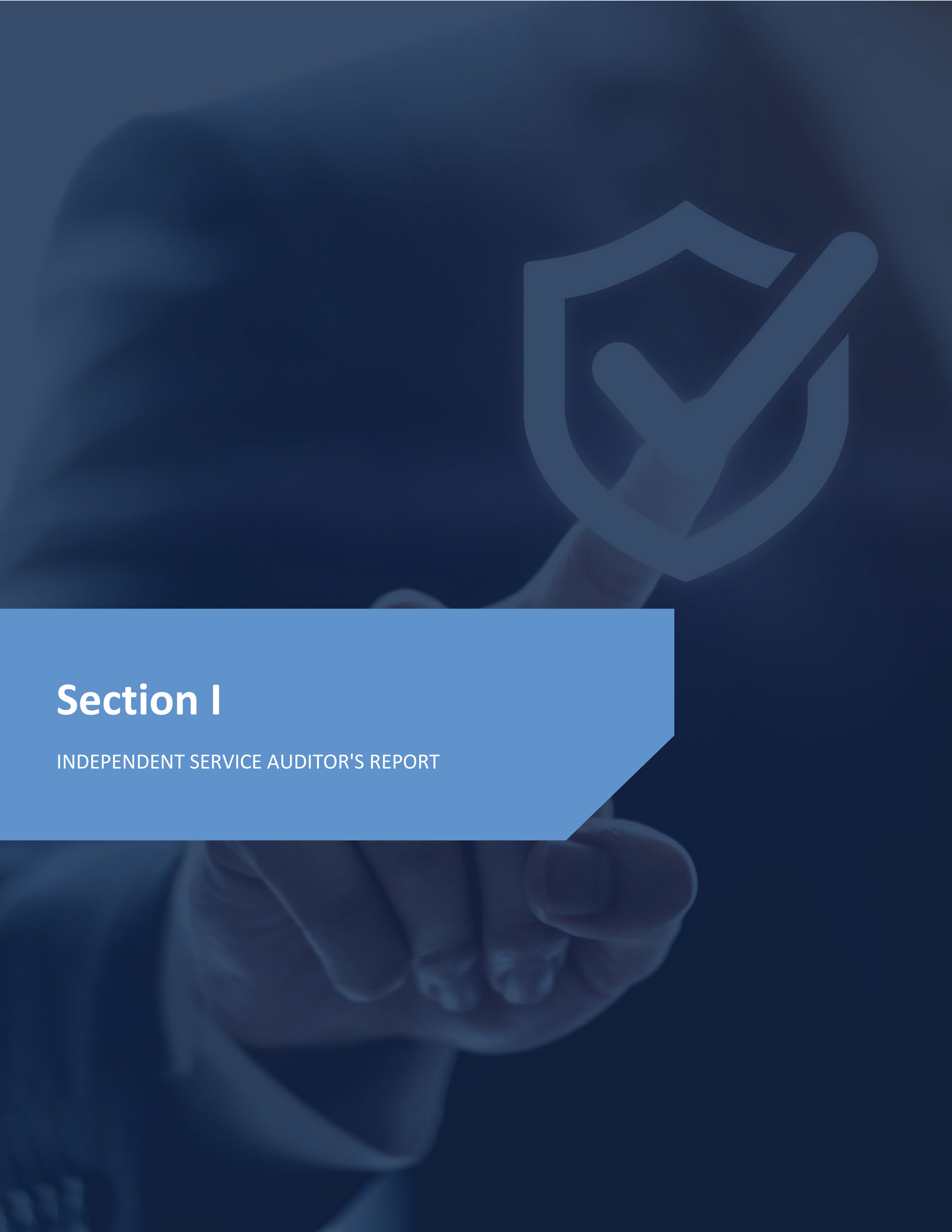
For the Period
August 13, 2024 to November 12, 2024

Together with Independent Service Auditor's Report

Report on Management's Description of

codeSMART

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

CodeSmart, Inc.

Scope

We have examined CodeSmart, Inc.’s accompanying description of its CodeSmart (system) titled “Description of CodeSmart” throughout the period August 13, 2024 to November 12, 2024 (description) based on the criteria for a description of a service organization’s system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 13, 2024 to November 12, 2024, to provide reasonable assurance that CodeSmart, 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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

CodeSmart, 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 CodeSmart, Inc., to achieve CodeSmart, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents CodeSmart, Inc.’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CodeSmart, 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 CodeSmart, Inc., to achieve CodeSmart, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents CodeSmart, Inc.’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CodeSmart, 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

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

An examination of 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 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 CodeSmart, Inc.’s CodeSmart (system) that was designed and implemented throughout the period August 13, 2024 to November 12, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period August 13, 2024 to November 12, 2024, to provide reasonable assurance that CodeSmart, 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 CodeSmart, Inc.’s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period August 13, 2024 to November 12, 2024, to provide reasonable assurance that CodeSmart, 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 CodeSmart, 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 CodeSmart, Inc.; user entities of CodeSmart, Inc.'s CodeSmart during some or all of the period August 13, 2024 to November 12, 2024, business partners of CodeSmart, Inc. subject to risks arising from interactions with the CodeSmart, 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
January 27, 2025

Section II

ASSERTION OF CODESMART, INC. MANAGEMENT

We have prepared the accompanying description of CodeSmart, Inc.'s "Description of CodeSmart" for the period August 13, 2024 to November 12, 2024, (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about CodeSmart, Inc.'s CodeSmart (system) that may be useful when assessing the risks arising from interactions with CodeSmart, Inc.'s system, particularly information about system controls that CodeSmart, 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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

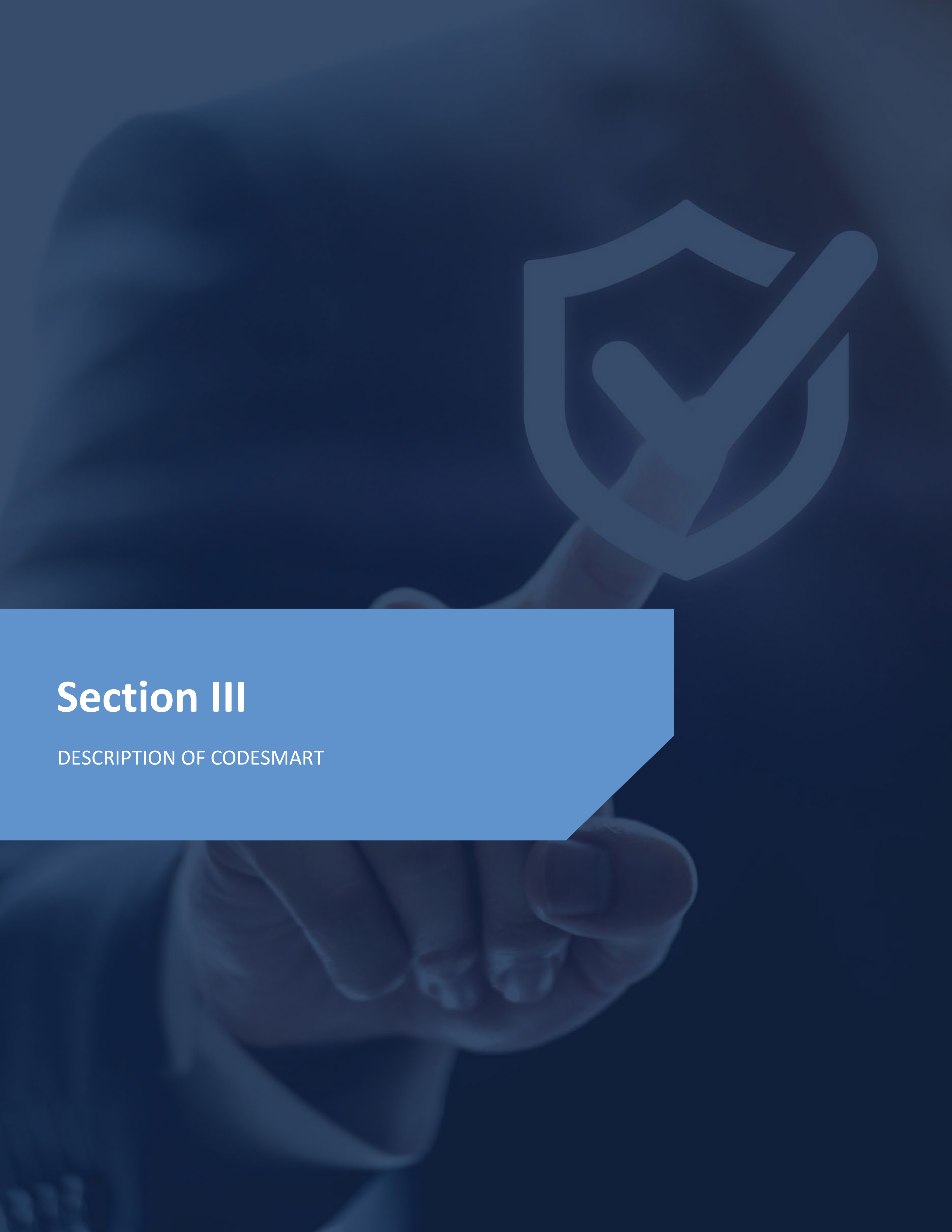
CodeSmart, Inc. uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CodeSmart, Inc., to achieve CodeSmart, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents CodeSmart, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CodeSmart, 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 CodeSmart, Inc., to achieve CodeSmart, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents CodeSmart, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CodeSmart, Inc.'s controls.

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

a. The description presents CodeSmart, Inc.'s CodeSmart (system) that was designed and implemented throughout the period August 13, 2024 to November 12, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period August 13, 2024 to November 12, 2024, to provide reasonable assurance that CodeSmart, 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 CodeSmart, Inc.'s controls throughout that period.
c. The controls stated in the description operated effectively throughout the period August 13, 2024 to November 12, 2024, to provide reasonable assurance that CodeSmart, 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 CodeSmart, Inc.'s controls operated effectively throughout that period.

CodeSmart, Inc. Management
January 27, 2025



Section III

DESCRIPTION OF CODESMART

COMPANY BACKGROUND

CodeSmart Inc. has been locally owned and operated in Washington since June 2002. We developed custom IT solutions tailored to meet the needs of our clients.

The staff at CodeSmart develops custom IT solutions. They manage analyze, design, develop, and deliver full end-to-end information systems. They apply Microsoft Azure, AWS CSP, Application development, and Infrastructure services by using IaC, conducting Well-Architected Framework Reviews with Microsoft Azure & AWS with good coding standards, and using recommended Microsoft & AWS best practices to produce successful information systems and projects. Our IT solutions include documentation to expedite knowledge transfer to our clients as well as maintain and enhance the system by consistently delivering quality solutions.

SERVICES PROVIDED

CodeSmart Inc. has developed an OCR (Optical Character Recognition) solution for HCA ECM and provide Operations & Maintenance support. The company also maintains the application for oCourt providing both Day 1 (Development) & Day 2 (Operations & Maintenance) services. This application simplifies data synchronization from supported cloud data to oCourt WA, automatically syncing data on a regular schedule, notifying users of any issues, and providing monitoring capabilities for tracking volume and types of changes.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

CodeSmart Inc. designs its processes and procedures related to its platform to meet its objectives for Consulting/Implementation services. Those objectives are based on the service commitments that CodeSmart Inc. makes to user entities, the laws and regulations that govern the provision of CodeSmart Inc. services, and the financial, operational, and compliance requirements that CodeSmart Inc. has established for the services. The Consulting Services/Implementation services of CodeSmart Inc. are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which CodeSmart Inc. operates.

Security 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 offered online.

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

- Security principles within the fundamental designs of the CodeSmart Inc. platform are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Designing, developing & maintaining Well Architected Frameworks deployed in both Azure & AWS
- Conducting SAST & DAST for the applications deployed by CodeSmart Inc.
- Regular Security Audits and Assessments: Conduct periodic security audits and assessments to identify and mitigate vulnerabilities, ensuring the platform remains secure against emerging threats.
- Incident Response and Management: Establishing a robust incident response plan to promptly address and manage security incidents, minimizing impact on operations and customer data.
- Access Control and Identity Management: Implementing strong access control measures and identity management protocols to ensure that only authorized personnel can access sensitive information and systems.
- Continuous Monitoring and Threat Detection: Utilizing advanced monitoring tools and threat detection systems to continuously monitor for suspicious activities and potential security breaches.
- Patch Management: Ensuring timely application of patches and updates to all systems and software to protect against known vulnerabilities.
- Data Backup and Recovery: Implementing robust data backup and recovery procedures to ensure data integrity and availability in the event of a disaster or data loss incident.
- Third-Party Vendor Management: Assessing and managing the security practices of third-party vendors and partners to ensure they meet the same security standards as CodeSmart Inc.

- Multi-Factor Authentication (MFA): Enforcing the use of multi-factor authentication to add an extra layer of security for user access to critical systems and data.
- Network Security: Implementing network security measures such as firewalls, intrusion detection/prevention systems, and secure VPNs to protect the integrity of network traffic.

CodeSmart Inc. establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in CodeSmart Inc. system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the CodeSmart Inc. platform.

COMPONENTS OF THE SYSTEM

Infrastructure

The primary infrastructure used to provide CodeSmart Inc. Services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Cloud	AWS Cloud Platform	Container runtime for web services, APIs, workers, and schedulers. Includes right scaling and self-healing to replace failed containers.
AWS Cloud	AWS Code Pipeline	CI/CD system to produce containers from source code and build packs, perform unit and integration tests on built containers, and deploy containers to staging and production environments.
AWS Cloud	AWS RDS Postgres	Primary transactional database with HA failover to hot standby and automatic backups.
AWS Cloud	Various Services, including VPC, Elastic IP, IAM, Lambda, Fargate, Classic Load Balancer	Proxies for outbound data warehouse connections from CodeSmart Inc. containers that allow all CodeSmart Inc. traffic to emanate from a set of stable IP addresses. This allows CodeSmart Inc. customers to add our IP addresses to an allowlist for their data warehouses.
AWS Cloud	S3	Temporary storage for customer data files unloaded from Redshift, and PostgreSQL.

Software

The primary software used to provide CodeSmart Inc.'s Services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Python	Linux	Primary development language/runtime for all CodeSmart Inc. applications.
Cloud Development Kit	Linux	Development of the OCR and Provider directory workflows for HCA.
PostgreSQL	Linux	Transactional database for CodeSmart Inc. data.
Amazon State Language	Amazon Managed	Job orchestration for OCR.

People

CodeSmart Inc. employees and contractors are organized into 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.

- Product Development: Product managers and software engineers who design and maintain the CodeSmart Inc. sync product, including the web interface, the proprietary sync engine, the job queuing infrastructure, and all debugging tools. This team designs and implements new CodeSmart Inc. functionality, assesses, and remediates any issues or bugs found in the CodeSmart Inc. product, and architects and deploys the underlying cloud infrastructure on which CodeSmart Inc. runs. This team also implements new data warehouse and SaaS connections for the CodeSmart Inc. sync engine. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team.

- Product Operations: The monitoring and maintenance of the CodeSmart Inc. product (once deployed) is handled by the operations role, which involves proactively designing and deploying monitoring software and tools to help identify errors or bugs in the CodeSmart Inc. product and remediate them either directly or via feedback to the product team. The operations team responds to alerts generated by our system, identifies issues with both CodeSmart Inc.'s sync engine and the configurations and SQL queries created by CodeSmart Inc. customers, and determines the best path to resolution. Operators also ensure that syncs are performing optimally (with high throughput and low latency) and that CodeSmart Inc. is using the correct cloud infrastructure and scale to maintain high sync performance. Finally, operators are responsible for responding to any potential security issues with CodeSmart Inc. and notifying affected customers if applicable.

- Commercial: Individuals with commercial roles work to market, sell, and support CodeSmart Inc. software. They are usually the primary point of contact for CodeSmart Inc. customers. They help identify which parts of the CodeSmart Inc. system are most useful to prospective customers, and what new product development or new sync connections need to be engineered to meet customer needs. In the marketing role, CodeSmart Inc. employees identify best practices for automating business operations and provide that information to CodeSmart Inc. customers and prospective customers via webinars, blog posts, white papers, and other channels. Finally, the CodeSmart Inc. customer success team ensures that CodeSmart Inc. customers can use the product effectively and without errors, by assisting CodeSmart Inc. customers with onboarding into the product, helping identify useful data sources and author SQL models, and proactively identifying any issues or bugs that occur when users try to sync their data.

Data

There are three major types of data used by CodeSmart Inc.:

- **Configuration Data**: Data used to configure HCA OCR functionality CodeSmart Inc.
- **Customer Data**: Data owned by HCA that CodeSmart Inc. receives as an extract from Enterprise Data Warehouse, processes it and shares it via secured API's to SaaS based application.
- **Log Data**: Logs, traces, and samples produced by the CodeSmart Inc. OCR will be captured in AWS CloudWatch

Configuration Data is stored in CodeSmart Inc.'s primary FHIR R4 Health Lake Database and includes:

- CodeSmart Inc. customers' email addresses, names, and company names.
- Credentials for accessing data warehouses, SaaS applications, and source code repositories, including usernames, passwords, OAuth tokens, and certificates.
- The names of databases, schemata, tables, columns, custom objects, and custom fields in customers' data warehouses and SaaS applications
- Configuration objects that determine how data is copied between systems, including field mappings, update policies, and schedules.
- Models (SQL queries) stored in CodeSmart Inc. by customers to provide logical views over data before being synced.
- Audit logs covering changes to each of the above items.

Configuration Data is treated as sensitive by CodeSmart Inc. It is stored in encrypted S3 buckets maintained by CodeSmart employees with RBAC configured. CodeSmart Inc. operators may access configuration data to troubleshoot customer issues or to gather feedback for improving the CodeSmart Inc.

Customer Data is the most sensitive data in the CodeSmart Inc. system, and CodeSmart Inc. stores it in encrypted S3 buckets. CodeSmart Inc. operators are permitted to access customer data to debug complex failures in the sync engine as a result of operational issues but are encouraged to use other tools and data sources to do this debugging when possible.

Log Data is produced by the OCR engine (Lambda, StepFunctions, APIGatway) which is eventually stored in CloudWatch log groups to make it easier for CodeSmart Inc. operators to monitor the health of the system and track down any issues. Log data is a trace of the actions performed by the system in the course of invoking the OCR API from the SaaS application. Log data will include snapshots of **Configuration Data** at the time the OCR API is called and CloudWatch has captured it, so operators can see what OCR API was attempting to be called and the respective configuration data. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include **Customer Data** captured by automatic tracers. CodeSmart Inc. endeavors to “scrub” logs of any **Customer Data** before they are persisted.

All data types processed by CodeSmart Inc. are encrypted on the wire – no networking connections used by CodeSmart Inc. for any purpose will ever send unencrypted data. In addition, all **Configuration Data** and **Log Data**, as well as samples of **Customer Data** stored by CodeSmart Inc. are encrypted at rest, by using industry-standard encryption algorithms provided by AWS.

PROCESSES AND PROCEDURES

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the CodeSmart Inc. policies and procedures that define how services should be delivered. These are located on the Company’s intranet and can be accessed by any CodeSmart Inc. team member.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow CodeSmart Inc. employees physical access. At present, CodeSmart Inc. does not maintain any office space and all work is conducted remotely.

Logical Access

CodeSmart Inc. employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

CodeSmart Inc. infrastructure runs entirely on AWS cloud and SaaS-based systems, and as such the resources used by employees to perform their roles are accounts and permissions within those systems. An employee can have one of their access levels to a SaaS or cloud service:

- Administrator – can alter policies and provision or de-provision users.
- User – has full read/write access to the SaaS or cloud service (except for administration).
- No access.

We currently do not have “read-only” roles in our SaaS or cloud applications or finer-grained policies on roles within those applications to avoid administrative complexity and friction for employees.

Roles are reviewed on an annual basis by management and the security team to ensure the least privileged access.

CodeSmart Inc. identifies employees primarily by their O365 account which is tagged to Active Directory, which functions as our corporate directory and SSO provider. The CodeSmart Inc. password policy mandates that employees and contractors use their O365 accounts to sign in to SaaS and cloud tools when supported. When O365 sign-in is not available, employees may authenticate using a strong, unique password, which must be stored in an approved password manager.

The CodeSmart Inc. O365 tenant requires users to use a second factor for authentication. In addition, any SaaS applications used by the company that don’t use O365 sign-in must be configured to use a second factor when possible.

The management team is responsible for onboarding new employees. Management is responsible for provisioning O365 and other SaaS accounts as dictated by the employee’s role and performing a background check, and the employee is responsible for reviewing CodeSmart Inc.’s policies, completing security training, and successfully gaining access to provisioned accounts (as well as enrolling a device for second-factor authentication). These steps must be completed within 14 days of hire.

When an employee is terminated, management is responsible for removing or disabling all of the employee’s accounts within 3 days.

CodeSmart Inc. employees may use a company-provided computer to perform their duties or may elect to “bring their own” device if that device is approved by the security team. Any computer (company-owned or BYOD) on which a CodeSmart Inc. employee performs sensitive work must employ full-disk encryption and have an approved endpoint monitoring tool installed. On employee termination, management will ensure the return of company-owned devices and handle their de-provisioning or reprovisioning based on the company’s Asset Management policy.

Computer Operations - Backups

Customer data is backed up by the CodeSmart Inc. cloud operations team in respective cloud storage. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations - Availability

CodeSmart Inc. maintains an Incident Response Policy that gives any CodeSmart Inc. employee the ability to initiate a response to a potential security incident by notifying the internal security team through several channels and assisting in classifying the severity of the incident.

External parties (customers and third-party security researchers) are also given a channel to send encrypted incident reports and responsibly disclose potential issues to the CodeSmart Inc. security team.

Internally, the CodeSmart Inc. operations team monitors the health of all applications, including the CodeSmart Inc. web UI, sync engine, databases, and cloud storage. Monitoring includes the availability and performance of the web UI, the throughput and queuing latency of the job scheduler, and any faults or errors encountered by users while configuring CodeSmart Inc. or while their data is being synced by CodeSmart Inc. Critical incidents are routed to an on-call operator who is responsible for acknowledging within one hour; if there is no acknowledgment, the incident is escalated to the rest of the operations team.

CodeSmart Inc. employs 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 Control

CodeSmart Inc. 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

CodeSmart Inc. 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. Our PaaS simplifies our logical network configuration by providing an effective firewall around all the CodeSmart Inc. application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

Our PaaS provider also automates the provisioning and de-provisioning 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.

CodeSmart Inc. 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.

CodeSmart Inc. does not maintain a corporate network, intranet, or VPN, but instead opts to use SaaS and cloud applications hosted on the public internet and secured by TLS connections.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Services performed by CodeSmart. This report does not include the data center hosting services provided by AWS.

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 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.

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 CodeSmart Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of CodeSmart Inc.'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

CodeSmart Inc.'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 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 CodeSmart Inc. 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 CodeSmart Inc. 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 CodeSmart Inc. 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 as a whole.

Organization Structure and Assignment of Authority and Responsibility

CodeSmart Inc. is currently organized in a simple, flat structure in which all employees report directly to the CEO. As the team grows, management will elect to build an organizational structure that ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting upward and downward in the organizational hierarchy.

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 Procedures

CodeSmart Inc.'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 operates at maximum efficiency. CodeSmart Inc.'s human resources policies and practices relating 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 onboarding documentation such as ACH, W4, and Candidate Information forms on their first day of employment.
- Evaluations for each employee are performed annually.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

CodeSmart's risk assessment process identifies and manages risks that could potentially affect CodeSmart's ability to provide reliable and secure services to our customers. As part of this process, CodeSmart 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 Monthly, and tasks are incorporated into the regular CodeSmart 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 CodeSmart's system; as well as the nature of the components of the system result in risks that the criteria will not be met. CodeSmart 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, CodeSmart'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 an integral component of CodeSmart'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.

CodeSmart uses several information and communication channels internally to share information with management, employees, contractors, and customers. CodeSmart uses Teams and email as the primary internal and external communications channels. In addition, CodeSmart communicates with customers via phone software like Zoiper/VoIP system, teams, and Webex.

Structured data is communicated internally via our SaaS applications (finance information in our data warehouse and Stripe) and our project management tools (Linear). Finally, CodeSmart 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. CodeSmart'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

CodeSmart'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 CodeSmart'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 CodeSmart'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 IN THE LAST 12 MONTHS

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

INCIDENTS IN THE LAST 12 MONTHS

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applicable to CodeSmart's Services system.

SUBSERVICE ORGANIZATIONS

CodeSmart's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to CodeSmart's services to be solely achieved by CodeSmart control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of CodeSmart.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – AWS		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed-circuit television cameras (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

CodeSmart management, along with the subservice organization, 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, CodeSmart performs monitoring of the subservice organization controls, including the following procedures:

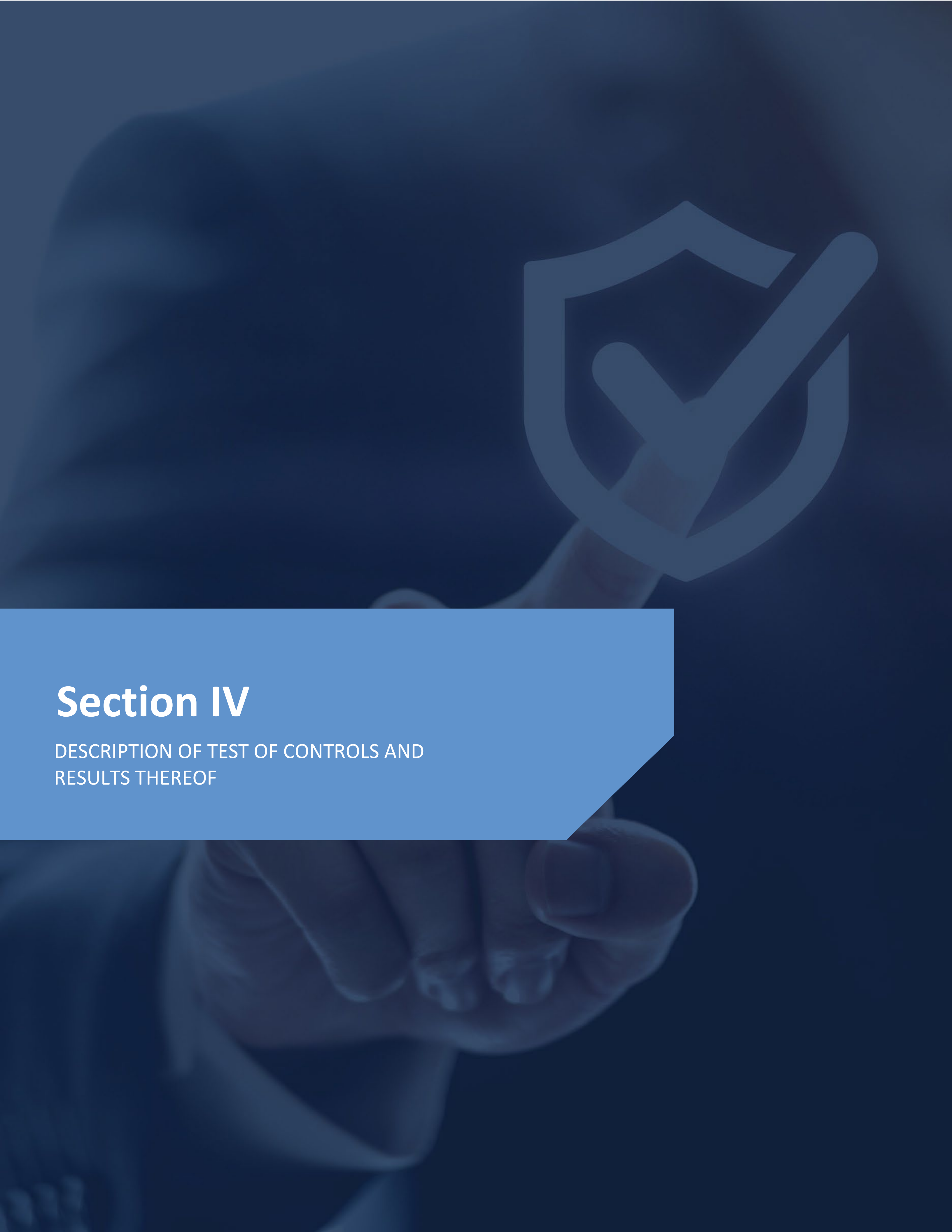
- Holding periodic discussions with vendors and subservice organizations.
- Reviewing attestation reports over services provided by vendors and subservice organizations.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

COMPLIMENTARY USER ENTITY CONTROLS

CodeSmart'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 CodeSmart's services to be solely achieved by CodeSmart control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of CodeSmart.

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 CodeSmart.
2. User entities are responsible for notifying CodeSmart 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 CodeSmart 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 CodeSmart services.
6. User entities are responsible for providing CodeSmart with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying CodeSmart 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 CodeSmart, 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 CodeSmart, 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 August 13, 2024 to November 12, 2024.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of CodeSmart, Inc. activities and operations, and inspection of CodeSmart, 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 CodeSmart, Inc. controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria for the Security Category	***Description of CodeSmart, 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.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected CodeSmart, Inc.'s Code of Conduct to determine that a policy outlines ethical expectations, behavior standards, and ramifications of noncompliance.	No exceptions noted.
	Internal personnel are evaluated via a formal performance review at least annually.	Inspected CodeSmart, Inc.'s sample of completed performance assessments to determine that internal personnel are evaluated via a formal performance review at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the performance evaluation/review was conducted outside of the review period on June 11, 12, and 14, 2024.
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected CodeSmart, Inc.'s Code of Conduct to determine that personnel who violate information security policies are subject to disciplinary action, and such disciplinary action is clearly documented in one or more policies.	No exceptions noted.
	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, 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 Board of Directors or equivalent entity function includes senior management and external advisors, who are independent of the company's operations. An information security team has also been established to govern cybersecurity.	Inspected CodeSmart, Inc.'s Board of Directors bylaws to determine that the Board of Directors or equivalent entity function includes senior management and external advisors, who are independent of the company's operations. An information security team has also been established to govern cybersecurity.	No exceptions noted.
	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	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.	The Board of Directors or equivalent entity function includes senior management and external advisors, who are independent of the company's operations. An information security team has also been established to govern cybersecurity.	Inspected CodeSmart, Inc.'s Board of Directors bylaws to determine that the Board of Directors or equivalent entity function includes senior management and external advisors, who are independent of the company's operations. An information security team has also been established to govern cybersecurity.	No exceptions noted.
	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	No exceptions noted.
	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.	Inspected CodeSmart, Inc.'s organization chart to determine that management maintains a formal chart to clearly identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	No exceptions noted.
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected CodeSmart, Inc.'s job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected CodeSmart, Inc.'s vendor SOC 2 reports to determine that they are collected and reviewed on at least an annual basis.	No exceptions noted.
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that new vendors are assessed in accordance with the policy prior to engaging with the vendor. Reassessment occurs at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no new vendors occurred during the review period.
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected CodeSmart, Inc.'s Code of Conduct to determine that a policy outlines ethical expectations, behavior standards, and ramifications of noncompliance.	No exceptions noted.
	Internal personnel are evaluated via a formal performance review at least annually.	Inspected CodeSmart, Inc.'s sample of completed performance assessments to determine that internal personnel are evaluated via a formal performance review at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the performance evaluation/review was conducted outside of the review period on June 11, 12, and 14, 2024.
	Background checks or their equivalent are performed before or promptly after a new hire's start date, as permitted by local laws.	Inspected CodeSmart, Inc.'s sample of background screening report to determine that background checks or their equivalent are performed before or promptly after a new hire's start date, as permitted by local laws.	No exceptions noted.
	Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	Inspected CodeSmart, Inc.'s sample of signed confidentiality agreements to determine that hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inspected CodeSmart, Inc.'s sample of completed security awareness training to determine that internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	No exceptions noted.
	An Information Security Policy establishes the security requirements for maintaining the security of applications, systems, infrastructure, and data.	Inspected CodeSmart, Inc.'s Information Security Policy to determine that a policy establishes the security requirements for maintaining the security of applications, systems, infrastructure, and data.	No exceptions noted.
	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected CodeSmart, Inc.'s Performance Review Policy to determine that a policy provides personnel context and transparency into their performance and career development processes.	No exceptions noted.
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected CodeSmart, Inc.'s vendor SOC 2 reports to determine that they are collected and reviewed on at least an annual basis.	No exceptions noted.
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	Internal personnel are evaluated via a formal performance review at least annually.	Inspected CodeSmart, Inc.'s sample of completed performance assessments to determine that internal personnel are evaluated via a formal performance review at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the performance evaluation/review was conducted outside of the review period on June 11, 12, and 14, 2024.
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected CodeSmart, Inc.'s control monitoring in Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
	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.	Inspected CodeSmart, Inc.'s organization chart to determine that management maintains a formal chart to clearly identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	No exceptions noted.
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected CodeSmart, Inc.'s Code of Conduct to determine that personnel who violate information security policies are subject to disciplinary action, and such disciplinary action is clearly documented in one or more policies.	No exceptions noted.
	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected CodeSmart, Inc.'s Performance Review Policy to determine that a policy provides personnel context and transparency into their performance and career development processes.	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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected CodeSmart, Inc.'s control monitoring in Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	An Information Security Policy establishes the security requirements for maintaining the security of applications, systems, infrastructure, and data.	Inspected CodeSmart, Inc.'s Information Security Policy to determine that a policy establishes the security requirements for maintaining the security of applications, systems, infrastructure, and data.	No exceptions noted.
	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected CodeSmart, Inc.'s vulnerability report to determine that vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	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.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected CodeSmart, Inc.'s website product page and network diagram to determine that descriptions of the company's services and systems are available to both internal personnel and external users.	No exceptions noted.
	A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected CodeSmart, Inc.'s website security and internal communication channel to determine that a confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	No exceptions noted.
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Inspected CodeSmart, Inc.'s Security Incident Response Plan to determine that a policy outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected CodeSmart, Inc.'s Network Security Policy to determine that a policy identifies the requirements for protecting information and systems within and across networks.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	No exceptions noted.
	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inspected CodeSmart, Inc.'s sample of completed security awareness training to determine that internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	No exceptions noted.
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected CodeSmart, Inc.'s job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	No exceptions noted.
	An infrastructure architecture and network diagram are maintained.	Inspected CodeSmart, Inc.'s data-flow diagram to determine that an infrastructure architecture and network diagram are maintained.	No exceptions noted.
	A SOC 2 system description provides an overview of an organization's control environment, including its background, services, IT infrastructure, people, processes, technologies, and controls.	Inspected CodeSmart, Inc.'s system description to determine that a SOC 2 system description provides an overview of an organization's control environment, including its background, services, IT infrastructure, people, processes, technologies, and controls.	No exceptions noted.
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected CodeSmart, Inc.'s website product page and network diagram to determine that descriptions of the company's services and systems are available to both internal personnel and external users.	No exceptions noted.
	Security commitments and expectations are communicated to both internal personnel and external users via the company's website.	Inspected CodeSmart, Inc.'s website security commitments to determine that security commitments and expectations are communicated to both internal personnel and external users via the company's website.	No exceptions noted.
	Terms of Service or the equivalent are published or shared with external users.	Inspected CodeSmart, Inc.'s terms of use to determine that Terms of Service or the equivalent are published or shared with external users.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Critical information is communicated to external parties, as applicable.	Inspected CodeSmart, Inc.'s external communications to determine that critical information is communicated to external parties, as applicable.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no critical external communications occurred during the review period.
	A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected CodeSmart, Inc.'s website security and internal communication channel to determine that a confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	No exceptions noted.
	A Privacy Policy is established for external users describing the company's privacy commitments.	Inspected CodeSmart, Inc.'s Privacy Policy to determine a policy is established for external users describing the company's privacy commitments.	No exceptions noted.
	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	No exceptions noted.
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that new vendors are assessed in accordance with the policy prior to engaging with the vendor. Reassessment occurs at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no new vendors occurred during the review period.
	An infrastructure architecture and network diagram are maintained.	Inspected CodeSmart, Inc.'s data-flow diagram to determine that an infrastructure architecture and network diagram are maintained.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, 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.	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	No exceptions noted.
	A 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. Risk tolerance and strategies are also defined in the policy.	Inspected CodeSmart, Inc.'s Risk Assessment and Treatment Policy to determine that a 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. Risk tolerance and strategies are also defined in the policy.	No exceptions noted.
	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
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.	A 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. Risk tolerance and strategies are also defined in the policy.	Inspected CodeSmart, Inc.'s Risk Assessment and Treatment Policy to determine that a 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. Risk tolerance and strategies are also defined in the policy.	No exceptions noted.
	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that a risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No exceptions noted.
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that new vendors are assessed in accordance with the policy prior to engaging with the vendor. Reassessment occurs at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no new vendors occurred during the review period.
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected CodeSmart, Inc.'s vulnerability report to determine that vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	No exceptions noted.
CC 3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that new vendors are assessed in accordance with the policy prior to engaging with the vendor. Reassessment occurs at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no new vendors occurred during the review period.

Trust Services Criteria for the Security Category	***Description of CodeSmart, 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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected CodeSmart, Inc.'s control monitoring in Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected CodeSmart, Inc.'s vulnerability report to determine that vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	No exceptions noted.
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.	Senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Inspected CodeSmart, Inc.'s Board of Directors meeting minutes and agenda to determine that senior management and/or Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	No exceptions noted.
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected CodeSmart, Inc.'s control monitoring in Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected CodeSmart, Inc.'s vulnerability report to determine that vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
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.	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that a policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected CodeSmart, Inc.'s Secure Development Policy to determine that a policy defines the requirements for secure software and system development and maintenance.	No exceptions noted.
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected CodeSmart, Inc.'s control monitoring in Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected CodeSmart, Inc.'s job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected CodeSmart, Inc.'s Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	Inspected CodeSmart, Inc.'s Encryption and Key Management Policy to determine that a policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	No exceptions noted.
	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected CodeSmart, Inc.'s Business Continuity and Disaster Recovery Plan to determine that the policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	No exceptions noted.
	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected CodeSmart, Inc.'s Data Classification Policy to determine that a policy details the security and handling protocols for sensitive data.	No exceptions noted.
	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inspected CodeSmart, Inc.'s Data Retention and Disposal Policy to determine that a policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	No exceptions noted.
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected CodeSmart, Inc.'s Configuration and Asset Management Policy to determine that a policy governs configurations for new sensitive systems.	No exceptions noted.
	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected CodeSmart, Inc.'s Change Management Policy to determine that a policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No exceptions noted.
	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected CodeSmart, Inc.'s Secure Development Policy to determine that a policy defines the requirements for secure software and system development and maintenance.	No exceptions noted.
	A Privacy Policy is established for external users describing the company's privacy commitments.	Inspected CodeSmart, Inc.'s Privacy Policy to determine a policy is established for external users describing the company's privacy commitments.	No exceptions noted.
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Inspected CodeSmart, Inc.'s Security Incident Response Plan to determine that a policy outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected CodeSmart, Inc.'s Network Security Policy to determine that a policy identifies the requirements for protecting information and systems within and across networks.	No exceptions noted.
	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected CodeSmart, Inc.'s control monitoring in Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
	An Acceptable Use Policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	Inspected CodeSmart, Inc.'s Acceptable Use Policy to determine that a policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	No exceptions noted.
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected CodeSmart, Inc.'s Code of Conduct to determine that personnel who violate information security policies are subject to disciplinary action, and such disciplinary action is clearly documented in one or more policies.	No exceptions noted.
	An Information Security Policy establishes the security requirements for maintaining the security of applications, systems, infrastructure, and data.	Inspected CodeSmart, Inc.'s Information Security Policy to determine that a policy establishes the security requirements for maintaining the security of applications, systems, infrastructure, and data.	No exceptions noted.
	An 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.	Inspected CodeSmart, Inc.'s Internal Control Policy to determine that a policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected CodeSmart, Inc.'s Performance Review Policy to determine that a policy provides personnel context and transparency into their performance and career development processes.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	Policies and procedures are reviewed and updated by management at least annually.	Inspected CodeSmart, Inc.'s Policy Packet to determine that policies and procedures are reviewed and updated by management at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the policies and procedures review was conducted outside of the review period on April 2024.
	Internal personnel review and accept applicable information security policies at least annually.	Inspected CodeSmart, Inc.'s sample of employees' acceptance of the policy to determine that internal personnel review and accept applicable information security policies at least annually.	No exceptions noted.
	Roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected CodeSmart, Inc.'s job descriptions to determine that roles and responsibilities related to security for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	No exceptions noted.
	A 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. Risk tolerance and strategies are also defined in the policy.	Inspected CodeSmart, Inc.'s Risk Assessment and Treatment Policy to determine that a 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. Risk tolerance and strategies are also defined in the policy.	No exceptions noted.
	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that a policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.
	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected CodeSmart, Inc.'s Vulnerability and Patch Management Policy to determine that a policy outlines the processes to efficiently respond to identified vulnerabilities.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
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.	A list of system assets, components, and respective owners is maintained and reviewed at least annually.	Inspected CodeSmart, Inc.'s system access to determine that a list of system assets, components, and respective owners are maintained and reviewed at least annually.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and the review was done outside the audit period in Dec 2024.
	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected CodeSmart, Inc.'s vendor access list to determine that personnel are assigned unique IDs to access sensitive systems, networks, and information.	No exceptions noted.
	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected CodeSmart, Inc.'s password policy and configuration to determine that personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	No exceptions noted.
	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected CodeSmart, Inc.'s Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected CodeSmart, Inc.'s vendor access list to determine that non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	No exceptions noted.
	Service data is encrypted at rest.	Inspected CodeSmart, Inc.'s data encryption to determine that service data is encrypted at rest.	No exceptions noted.
	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	Inspected CodeSmart, Inc.'s Encryption and Key Management Policy to determine that a policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	No exceptions noted.
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected CodeSmart, Inc.'s Configuration and Asset Management Policy to determine that a policy governs configurations for new sensitive systems.	No exceptions noted.
	Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Inspected CodeSmart, Inc.'s device settings and configuration to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected CodeSmart, Inc.'s Network Security Policy to determine that configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	No exceptions noted.
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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected CodeSmart, Inc.'s Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected CodeSmart, Inc.'s role-based access control to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	No exceptions noted.
	Users are provisioned access to systems based on the principle of least privilege.	Inspected CodeSmart, Inc.'s role-based access control to determine that users are provisioned access to systems based on the principle of least privilege.	No exceptions noted.
	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected CodeSmart, Inc.'s sample of completed access revocation to determine that upon termination or when internal personnel no longer require access, system access is removed, as applicable.	No exceptions noted.
	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate that internal user access is commensurate with job responsibilities.	Inspected CodeSmart, Inc.'s access review to determine that system owners conduct scheduled user access reviews of production servers, databases, and applications to validate that internal user access is commensurate with job responsibilities.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and the review was done outside the audit period in Dec 2024.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected CodeSmart, Inc.'s Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected CodeSmart, Inc.'s vendor access list to determine that non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	No exceptions noted.
	Users are provisioned access to systems based on the principle of least privilege.	Inspected CodeSmart, Inc.'s role-based access control to determine that users are provisioned access to systems based on the principle of least privilege.	No exceptions noted.
	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected CodeSmart, Inc.'s sample of completed access revocation to determine that upon termination or when internal personnel no longer require access, system access is removed, as applicable.	No exceptions noted.
	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate that internal user access is commensurate with job responsibilities.	Inspected CodeSmart, Inc.'s access review to determine that system owners conduct scheduled user access reviews of production servers, databases, and applications to validate that internal user access is commensurate with job responsibilities.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and the review was done outside the audit period in Dec 2024.
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 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.
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.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected CodeSmart, Inc.'s vendor SOC 2 reports to determine that they are collected and reviewed on at least an annual basis.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected CodeSmart, Inc.'s password policy and configuration to determine that personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	No exceptions noted.
	Service data transmitted over the internet is encrypted in transit.	Inspected CodeSmart, Inc.'s encryption in transit for the web application to determine that service data transmitted over the internet is encrypted in transit.	No exceptions noted.
	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	Inspected CodeSmart, Inc.'s Encryption and Key Management Policy to determine that a policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	No exceptions noted.
	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected CodeSmart, Inc.'s monitoring and security tools to determine that they are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.
	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected CodeSmart, Inc.'s Network Security Policy to determine that configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	No exceptions noted.
	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected CodeSmart, Inc.'s Network Security Policy to determine that a policy identifies the requirements for protecting information and systems within and across networks.	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.	Service data is encrypted at rest.	Inspected CodeSmart, Inc.'s data encryption to determine that service data is encrypted at rest.	No exceptions noted.
	Service data transmitted over the internet is encrypted in transit.	Inspected CodeSmart, Inc.'s encryption in transit for the web application to determine that service data transmitted over the internet is encrypted in transit.	No exceptions noted.
	Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Inspected CodeSmart, Inc.'s device settings and configuration to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	An Acceptable Use Policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	Inspected CodeSmart, Inc.'s Acceptable Use Policy to determine that a policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected CodeSmart, Inc.'s baseline configurations and version control tool system to determine that configurations and codebases for production infrastructure, systems, and applications are securely managed.	No exceptions noted.
	Software changes are tested prior to being deployed into production.	Inspected CodeSmart, Inc.'s software changes to determine that they are tested prior to being deployed into production.	No exceptions noted.
	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected CodeSmart, Inc.'s change tracking and approval process to determine that system changes are approved by at least 1 independent person prior to deployment into production.	No exceptions noted.
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected CodeSmart, Inc.'s Configuration and Asset Management Policy to determine that a policy governs configurations for new sensitive systems.	No exceptions noted.
	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected CodeSmart, Inc.'s Change Management Policy to determine that a policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No exceptions noted.
	Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Inspected CodeSmart, Inc.'s device settings and configuration to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	No exceptions noted.
	An Acceptable Use Policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	Inspected CodeSmart, Inc.'s Acceptable Use Policy to determine that a policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected CodeSmart, Inc.'s baseline configurations and version control tool system to determine that configurations and codebases for production infrastructure, systems, and applications are securely managed.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected CodeSmart, Inc.'s Configuration and Asset Management Policy to determine that a policy governs configurations for new sensitive systems.	No exceptions noted.
	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected CodeSmart, Inc.'s monitoring and security tools to determine that they are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.
	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, and unusual system activity, and monitor system performance, as applicable.	Inspected CodeSmart, Inc.'s monitoring tools to determine that logging and monitoring software is used to collect data from infrastructure to detect potential security threats, and unusual system activity, and monitor system performance, as applicable.	No exceptions noted.
	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected CodeSmart, Inc.'s Vulnerability and Patch Management Policy to determine that a policy outlines the processes to efficiently respond to identified vulnerabilities.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected CodeSmart, Inc.'s vulnerability report to determine that vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	No exceptions noted.
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.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected CodeSmart, Inc.'s monitoring and security tools to determine that they are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.
	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, and unusual system activity, and monitor system performance, as applicable.	Inspected CodeSmart, Inc.'s monitoring tools to determine that logging and monitoring software is used to collect data from infrastructure to detect potential security threats, and unusual system activity, and monitor system performance, as applicable.	No exceptions noted.
	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected CodeSmart, Inc.'s Network Security Policy to determine that a policy identifies the requirements for protecting information and systems within and across networks.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Inspected CodeSmart, Inc.'s Security Incident Response Plan to determine that a policy outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected CodeSmart, Inc.'s security incident log template to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security incidents occurred during the review period.
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.	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected CodeSmart, Inc.'s Business Continuity and Disaster Recovery Plan to determine that the policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	No exceptions noted.
	Critical information is communicated to external parties, as applicable.	Inspected CodeSmart, Inc.'s external communications to determine that critical information is communicated to external parties, as applicable.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no critical external communications occurred during the review period.
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Inspected CodeSmart, Inc.'s Security Incident Response Plan to determine that a policy outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected CodeSmart, Inc.'s security incident log template to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security incidents occurred during the review period.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve the company's security and operations.	Inspected CodeSmart, Inc.'s security incident notifications to determine that after any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve the company's security and operations.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security incidents occurred during the review period.
	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Inspected CodeSmart, Inc.'s Disaster Recovery Testing to determine that the Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the tabletop exercise was conducted outside of the review period on November 26, 2024.
	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected CodeSmart, Inc.'s Code of Conduct to determine that personnel who violate information security policies are subject to disciplinary action, and such disciplinary action is clearly documented in one or more policies.	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Inspected CodeSmart, Inc.'s Disaster Recovery Testing to determine that the Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the tabletop exercise was conducted outside of the review period on November 26, 2024.
	Critical information is communicated to external parties, as applicable.	Inspected CodeSmart, Inc.'s external communications to determine that critical information is communicated to external parties, as applicable.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no critical external communications occurred during the review period.

Trust Services Criteria for the Security Category	*Description of CodeSmart, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Inspected CodeSmart, Inc.'s Security Incident Response Plan to determine that a policy outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected CodeSmart, Inc.'s security incident log template to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security incidents occurred during the review period.
	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve the company's security and operations.	Inspected CodeSmart, Inc.'s security incident notifications to determine that after any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve the company's security and operations.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security incidents occurred during the review period.
	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Inspected CodeSmart, Inc.'s Disaster Recovery Testing to determine that the Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that the tabletop exercise was conducted outside of the review period on November 26, 2024.
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.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected CodeSmart, Inc.'s vendor access list to determine that on-console access to production infrastructure is restricted to users with a unique SSH key or access key.	No exceptions noted.
	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected CodeSmart, Inc.'s baseline configurations and version control tool system to determine that configurations and codebases for production infrastructure, systems, and applications are securely managed.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	Software changes are tested prior to being deployed into production.	Inspected CodeSmart, Inc.'s software changes to determine that they are tested prior to being deployed into production.	No exceptions noted.
	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected CodeSmart, Inc.'s change tracking and approval process to determine that system changes are approved by at least 1 independent person prior to deployment into production.	No exceptions noted.
	Development, staging, and production environments are segregated.	Inspected CodeSmart, Inc.'s environment segregation to determine that development, staging, and production environments are segregated.	No exceptions noted.
	Production data is not used in the development and testing environments unless required for debugging customer issues.	Inspected CodeSmart, Inc.'s Change Management and Secure Development Policy to determine that production data is not used in the development and testing environments unless required for debugging customer issues.	No exceptions noted.
	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected CodeSmart, Inc.'s Configuration and Asset Management Policy to determine that a policy governs configurations for new sensitive systems.	No exceptions noted.
	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected CodeSmart, Inc.'s Change Management Policy to determine that a policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No exceptions noted.
	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected CodeSmart, Inc.'s Secure Development Policy to determine that a policy defines the requirements for secure software and system development and maintenance.	No exceptions noted.
Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected CodeSmart, Inc.'s Business Continuity and Disaster Recovery Plan to determine that the policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	No exceptions noted.
	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Inspected CodeSmart, Inc.'s Security Incident Response Plan to determine that a policy outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
	Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events.	Inspected CodeSmart, Inc.'s cybersecurity insurance policy to determine that it has been procured to help minimize the financial impact of cybersecurity loss events.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of CodeSmart, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	A 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. Risk tolerance and strategies are also defined in the policy.	Inspected CodeSmart, Inc.'s Risk Assessment and Treatment Policy to determine that a 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. Risk tolerance and strategies are also defined in the policy.	No exceptions noted.
	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected CodeSmart, Inc.'s completed risk assessment to determine that a risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No exceptions noted.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected CodeSmart, Inc.'s Vendor Management Policy to determine that a policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.
	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected CodeSmart, Inc.'s vendor SOC 2 reports to determine that they are collected and reviewed on at least an annual basis.	No exceptions noted.