



SMTDATA

SMT Data

SOC 2 Type II Report

Description of the SMT Data System

Controls Relevant to **Security**

For the Period July 1 2024 to September 30 2024

With Independent Service Auditor's Report
Including Tests Performed and Results thereof

DECRYPT

COMPLIANCE



Table of Contents

I. SMT Data’s Management Assertion.....	4
II. Independent Service Auditor’s Report.....	6
III. SMT Data’s Description of the SMT Data System.....	11
Company & System Overview and Background.....	11
Overview of the Company’s Internal Controls.....	13
Risk Assessment.....	15
Penetration Testing.....	17
Logical and Physical Access.....	18
System Access.....	19
Software Development Lifecycle (SDLC) Overview.....	20
Description of the Production Environment.....	21
Security and Architecture.....	22
Support.....	25
Changes to the System after the Examination Period.....	26
System Incidents.....	26
Complementary User Entity Controls (CUEC).....	26
Subservice Organizations Carved-Out Controls: AWS.....	27
IV. Description of Criteria, Controls, Tests, and Results of Tests.....	29
Testing performed and results of tests of entity level controls.....	29
Control criteria and related controls for systems and applications.....	29
SMT Data Controls and related Trust Services Criteria.....	30
Description of Test of Controls and Results.....	36
Security Category.....	36



Section I Management Assertion

I. SMT Data's Management Assertion

We have prepared the accompanying "SMT Data's Description of the SMT Data System" (Description) of ("Service Organization") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the SMT Data System (System) that may be useful when assessing the risks arising from interactions with the System throughout the period July 1, 2024 to September 30, 2024, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Complementary subservice organization controls: SMT Data A/S uses a subservice organization for cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SMT Data, to achieve SMT Data's service commitments and system requirements based on the applicable trust services criteria. The Description presents SMT Data's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SMT Data's controls. The Description does not disclose the actual controls at the subservice organization.

Complementary user entity controls: The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of SMT Data controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

- (a) The Description presents the System that was designed and implemented throughout the period July 1, 2024 to September 30, 2024 in accordance with the Description Criteria
- (b) The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls assumed in the design of SMT Data's controls throughout the period July 1, 2024 to September 30, 2024
- (c) The SMT Data controls stated in the Description operated effectively throughout the period July 1, 2024 to September 30, 2024 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls assumed in the design of SMT Data's controls throughout the period July 1, 2024 to September 30, 2024

SMT Data
November 20, 2024

Section II

Independent Service Auditor's Report

Section III

SMT Data's Description of the SMT Data System

III. SMT Data's Description of the SMT Data System

Company & System Overview and Background

SMT Data provides capacity management and performance analysis, we help larger companies with the performance of their IT infrastructure.

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting SMT Data Platform and does not extend to other available software products and services or the controls at third third-party service providers.

Products and Services offered by SMT Data's Platform

SMT Data offers IT Business Intelligence (ITBI™) which enables our customers to gather, understand, and optimize their IT capacity and performance costs on both mainframe and midrange platforms.

Organizational Structure

The company has defined structures, and reporting lines with assigned authority and responsibilities, in order to appropriately meet the security requirements:

Description of key personnel roles & responsibilities

C-level management:

- **CEO:** The CEO is responsible for providing strategic direction, financial oversight, and operational leadership. The CEO works closely with the board of directors and the executive team to ensure the company's growth, profitability, and sustainability.
- **CTO:** The CTO is responsible for leading and developing the DevOps team, overseeing product development, managing IT infrastructure, and ensuring compliance with security standards. They collaborate with the CEO and other stakeholders to align technology strategies with business goals, while driving innovation, technical leadership, and continuous improvement within the organization.
- **CCO:** The CCO's responsibilities and tasks for this role align with those outlined for the Regional Sales Manager.
- **CFO:** The CFO is responsible for overseeing the company's financial health, guiding its financial strategy and ensuring strong financial management. The CFO plays a critical role in budgeting, forecasting, and financial risk management.

Organizational Chart

SMT Data A/S

Chairman of the Board

CEO

Sales

CCO
 Regional Sales Manager
 Regional Sales Manager

ITBI Evangelists

Principal ITBI Evangelist
 ITBI Director

ITBI Services

Vice President of ITBI Services
 Senior ITBI Consultant / CISO
 Senior ITBI Consultant
 Senior ITBI Consultant
 Senior ITBI Consultant

DevOps

CTO
 IT Operations Consultant
 Development Manager
 Full Stack Engineer
 Developer
 Front End Developer
 Full Stack Engineer
 Lead Developer

F&A

CFO

MarCom

Digital Coordinator

©copyright - SMT Data, 2024

classifies and manages the inventory of information assets. The assets inventory is reviewed by the CTO on an annual basis.

Penetration Testing

An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner. High/Critical issues are investigated and dealt with as part of the SDLC process or by any necessary means. A re-test is performed, when necessary, to verify the remediation of the critical/high issues.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks. SMT Data's operating and functional units are required to implement control activities that help achieve business objectives associated with the following:

- Adherence to the organization's policies and procedures
- The effectiveness and efficiency of operations
- Compliance with applicable laws and regulations

The control activities are designed to address specific risks associated with SMT Data operations and are reviewed as part of the risk assessment process. SMT Data has developed formal policies and procedures covering various operational matters to document the requirements for the performance of many control activities.

Information and Communication

Information and communication are integral components of SMT Data's internal control system. They involve the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At SMT Data, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Internal communication

A detailed description of the product architecture and system boundaries is documented and available internally to the company's employees. Release notes are sent internally describing the closed stories that were part of new versions released. In addition, SMT Data's approved policies as well as the process of informing their customers and business partners about breaches of the system Security are communicated to personnel responsible for implementing them in the internal application. The company maintains an internal informational knowledge base describing the company's environment, its boundaries, user responsibilities and services.

External communication

New features are communicated to customers through the email to keep them updated on new product features on a quarterly basis. In addition, SMT Data's approved policies, as well as the process of informing their customers and business partners about breaches of the system Security, are communicated to personnel responsible for implementing them in the internal application. The company maintains external documentation describing the product features, system boundaries, user guides, and services commitments.

Logical and Physical Access

A security policy is documented by SMT Data management and is reviewed and approved on an annual basis. The access to the production server is performed using the two-factor authentication method. SMT Data has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission.

Access Control, User, and Permissions Management

Access to SMT Data information assets is restricted and The organization enforces and holds individual employees accountable for their internal control responsibilities, in line with their job objectives and KPIs. SMT Data employees and contractors will not be granted access to any information asset that is not directly needed for their work in SMT Data. The company manages access governance through a roles-based access control matrix based on the job description and responsibilities. User access and permissions are reviewed and approved by the company's management on a quarterly basis. Additionally, access authorization is defined based on work purposes only.

The company has established a formal standard for passwords to govern the management and use of authentication mechanisms. Strong password configuration settings, where applicable, are enabled, including:

- (1) Use a minimum of 8 characters
- (2) Use upper case, lower case, numeric, and special character values

Access to system resources is protected by means of the following security measures:

1. Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method.
2. The access to the production server is performed using the two-factor authentication method.
3. The company has an established key management process in place to support the organization's use of cryptographic techniques.

4. The company secures and controls its employees' devices to enforce security settings including - hard-disk encryption, auto patching, password requirement, auto screen-lock, remote wipe capabilities, antivirus and deployment of additional policies.

Provisioning of new user access must follow a notification from HR.

System Access

Production Environment Logical Access

The production environment access is protected and restricted.

User access and permissions are reviewed and approved by the company's management on a quarterly basis. The access to the production server is performed using the two-factor authentication method. Privileged access rights are defined as any access authorizations created for the employee for their work, temporarily or permanently, beyond those specified in respect of their position in the user permissions table. All access requests to organizational systems, including administrator accounts, are approved prior to access provisioning. Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method.

Backup Access

Access to alter and delete backups is restricted to authorized users and performed using two-factor authentication .

Source Control Access

Access to the source control tool is performed using two-factor authentication and is restricted to authorized personnel.

Application and External Database Access

Access to sensitive databases is restricted to authorized users and uses a VPN.

Identity Management Access

Access to the identity management tool is performed using two-factor authentication and is restricted to authorized personnel.

Remote Access

SMT Data operates using a fully cloud-native application and environment, and as such - remote access follows the same process as accessing organizational resources and systems in the physical office. Therefore, all SMT Data employees should be connected via the company password policy, and using the MFA mechanism shall be enforced as well, in order to enforce and ensure stringent security measures when connecting to SMT Data via a remote connection.

Physical Access and Visitors

Physical access to the offices is restricted to authorized personnel electronic identification cards. The ID card is needed within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities. While at SMT Data offices, employees are required to use key fobs to access the offices.. Visitors to SMT Data offices are required to be accompanied by a SMT Data employee at all times during their stay. Employees encountering an unfamiliar or suspicious person wandering around the office are expected to ask them politely about the nature of their business and if necessary, accompany them to their host. Visitors are not allowed to access or connect to SMT Data company's network or equipment.

Termination of Access

User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination. Additionally, upon leaving, organizational assets shall be returned.

Software Development Lifecycle (SDLC) Overview

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the change management application. Each change goes through a life cycle. Code changes must be reviewed and approved in order to progress through the SDLC and deploy a version to production. Request tickets are created to document change requests within the change management system. Pull requests and change tickets are linked to each other so the code change can be tracked.

Software Testing and QA Process: A successful test result is mandatory in order to continue with the SDLC process and deploy a version to the production environment. In cases of test failures, the build is stopped and does not deploy .

Segregation within the lifecycle: Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.

Monitoring the Change Management Processes

Changes that may affect system Security -related issues are communicated through emails to the different team owners. Changes are documented within the system and approved by authorized employees. The company developed a process in order to manage emergency changes. A post approval process is performed for each emergency change.

Network Infrastructure

The company has enabled multiple network security controls as SSH restriction, port restriction, and remote access restriction. Robust network infrastructure is essential for reliable and secure real-time data communication between SMT Data's cloud service components. To provide sufficient capacity, SMT Data's network infrastructure relies on platforms provided by AWS. To ensure appropriate network security levels, SMT Data security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring Security. SMT Data's security model encompasses the following components:

- Application layer security, including:
 - Various authentication schemas such as multi-factor authentication (MFA), unique ID, and complex password policy
 - Logical security
 - Penetration testing
 - IP address source restriction
 - Customers' data encryption at rest and in transit
- Network and infrastructure security, including
 - Network architecture
 - Risk management
 - AWS data centers
 - Cloud operation security (change management, monitoring, and log analysis)
 - Network vulnerability scanning
 - Intrusion detection/prevention systems

Web, Application, and Service-Supporting Infrastructure Environment

SMT Data utilizes the clustered infrastructure design of AWS to provide redundancy and high availability. In addition, the infrastructure is configured in a way that enables auto-scaling capabilities. This allows for supporting high performance during demand spikes for the services.

Production Monitoring

Actions performed in the production environment, including OS, DB, and application are monitored, logged, and reviewed. Audit trail (security logs) is deployed on the production environment continuously to capture actions made directly by the user or a cloud service. Audit trail security logs are configured to be retained for 365 days.

Security and Architecture

SMT Data provides a secure, reliable, and resilient Software-as-a-Service platform that has been designed based on industry best practices. The below addresses the network and hardware infrastructure, software, and information security elements that SMT Data delivers as part of this platform, database management system security, application controls, and intrusion detection monitoring software. Intrusion detection system scans continuously for potential security issues and

alerts the administrator upon discovering unexpected and potentially malicious activity in the production environment, with a high/critical risk rating.

A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring. Data restoration checks are performed on an annual basis in order to test and ensure the company's ability to recover from a security incident.

An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.

Data Center Security

SMT Data relies on the global infrastructure of AWS which can include the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards and regulations.

The environmental protection managed by the vendors' policies are:

- **Redundancy** - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- **Fire Detection and Suppression** - Automatic fire detection and suppression equipment have been installed to reduce risk.
- **Redundant Power** - the data center electrical power systems are designed to be fully redundant and maintainable without impact on operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure. Data centers use generators to provide backup power for the entire facility.
- **Climate and Temperature Controls** - maintain a constant operating temperature and humidity level for all hardware.
- **Physical access** - AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures, and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas.

Application Security

- **Penetration Testing** - The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.
- **Vulnerabilities Management** - Internal vulnerability scanning is performed by the relevant teams using sufficient tools. Production networks undergo vulnerability scans. A quarterly review is performed and issues identified are tracked and remediated in accordance with the

Incident Management Process

SMT Data has a defined and implemented Incident Management Policy. Within the policy, there are defined processes and procedures to be followed for respective incident types. The detailed Incident Management Policy includes and details the different phases of incident management and response, including the various response protocols - which detail the appropriate reporting and escalation procedures and personnel to contact for each respective incident type. Detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.

Escalation Process

SMT Data's goal is to resolve issues efficiently. The issue is tracked and updated in the support ticketing system. The escalation process is defined and documented by Customer Support. The company uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders by an internal communication tool, based on predefined rules. The notifications are reviewed and processed according to their level of urgency.

Changes to the System after the Examination Period

No significant changes have occurred to the services provided to user entities as of the date of this report.

System Incidents

No significant incidents have occurred to the service provided to user entities as of the date of this report.

Complementary User Entity Controls (CUEC)

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with SMT Data.
- Ensuring timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with SMT Data's services.
- Maintaining authorized, secure, timely, and complete transactions for user organizations relating to SMT Data's services.
- Protecting data that is sent to SMT Data by using appropriate methods to ensure security, and non-repudiation.
- Implementing controls requiring additional approval procedures for critical transactions relating to SMT Data's services.
- Reporting to SMT Data in a timely manner any material changes to their overall control environment that may adversely affect services being performed by SMT Data.

- Notifying SMT Data in a timely manner of any changes to personnel directly involved with services performed by SMT Data. This person may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by SMT Data.
- Adhering to the terms and conditions stated within their contracts with SMT Data.

Subservice Organizations Carved-Out Controls: AWS

The subservice organizations are expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict access to the virtual and physical servers, software, firewalls, and physical storage to authorized individuals and review the list of users and permissions on a regular basis.
- Implement controls to:
 - Provision access only to authorized persons.
 - Remove access when no longer appropriate.
 - Secure the facilities to permit access only to authorized persons.
 - Monitor access to the facilities.
- Be consistent with defined system security related to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, and related policies.
- Provide that only authorized tested and documented changes are made to the system.



Section IV Description of Criteria, Controls, Tests, and Results of Tests

IV. Description of Criteria, Controls, Tests, and Results of Tests

Testing performed and results of tests of entity level controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of SMT Data and the tests performed by Decrypt Compliance and results are the responsibility of the service auditor.

Control criteria and related controls for systems and applications

On the pages that follow, the applicable control criteria and the controls to achieve the criteria have been specified by, and are the responsibility of, SMT Data. The sections “Tests Performed by Decrypt Compliance” and “Results” are the responsibility of Decrypt Compliance PC.

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

- (1) inspected the source of the IPE,
- (2) inspected the query, script, or parameters used to generate the IPE,
- (3) tied data between the IPE and the source, and/or
- (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity.

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



SMT Data Controls and related Trust Services Criteria

Control #	Controls Specified by SMT Data	Related SOC 2 Criter
CC.01.01	The Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	CC1.1, CC1.2, CC2.2, CC2.3
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	CC1.3, CC2.2, CC4.1, CC4.2, CC5.1, CC5.2
CC.01.03	The company has defined structures, and reporting lines with assigned authority and responsibilities, in order to appropriately meet the security requirements.	CC1.3, CC2.2
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	CC1.4, CC2.1, CC2.2, CC4.1, CC4.2, CC5.2, CC5.3, CC6.8, CC8.1
CC.01.05	The company's employees are required to read and accept the Code of conduct, Acceptable use policy upon their hire. Management monitors employees' compliance with an official signature.	CC1.1, CC1.5
CC.01.07	The company conducts pre-employment screening checks of candidates commensurate with the employee's position and level, in accordance with local laws.	CC1.4
CC.01.08	New employees go through an onboarding process to be informed of their role responsibilities, organizational policies, and provision of relevant access.	CC1.4
CC.01.09	The company provides education and training to ensure that the skill sets and technical competency of employees are developed and maintained.	CC1.4
CC.01.10	The company performs an annual performance review of all employees that have been at the organization for 12 or more months. A formal evaluation of each employee is performed in alignment with the Company's objectives.	CC1.5
CC.02.01	A detailed description of the product architecture and system boundaries is documented	CC2.1, CC6.1

Control #	Controls Specified by SMT Data	Related SOC 2 Criter
CC.03.04	The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the CTO on an annual basis.	CC3.2, CC6.1
CC.04.01	An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.	CC4.1, CC7.1, CC7.2
CC.05.02	Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.	CC5.1, CC6.1 , CC8.1
CC.06.01	All access requests to organizational systems, including administrator accounts, is approved prior to access provisioning.	CC6.1, CC6.2, CC6.3
CC.06.02	The company manages access governance through a roles-based access control matrix based on the job description and responsibilities.	CC6.1, CC6.3
CC.06.03	The company has established a formal standard for passwords to govern the management and use of authentication mechanisms. Strong password configuration settings, where applicable, are enabled, including: (1) Use a minimum of 8 characters (2) Use upper case, lower case, numeric, and special character values	CC6.1
CC.06.05	Access to the identity management tool is performed using two-factor authentication and is restricted to authorized personnel.	CC6.1
CC.06.06	Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method.	CC6.1
CC.06.08	Access to sensitive databases is restricted to authorized users and uses a VPN.	CC6.1
CC.06.09	Access to the source control tool is performed using two-factor authentication and is restricted to authorized personnel.	CC6.1
CC.06.10	The access to the production server is performed using the two-factor authentication method.	CC6.1

Control #	Controls Specified by SMT Data	Related SOC 2 Criter
CC.08.05	Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated.	CC7.1, CC8.1
CC.08.07	A successful test result is mandatory in order to continue with the SDLC process and deploy a version to the production environment. In cases of test failures, the build is stopped and does not deploy.	CC8.1
CC.08.08	The company developed a process in order to manage emergency changes. A post approval process is performed for each emergency change.	CC8.1
CC.08.11	The company enforced segregation between development, staging, and production environments to enforce confidentiality and privacy of customers' data.	CC6.1, CC8.1
CC.09.02	The company assesses, on an annual basis, the risks that vendors and business partners represent to the achievement of the Company's objectives.	CC3.2, CC9.2
CC.09.04	The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	CC3.2, CC9.2
AV.03.02	Data restoration checks are performed continuously in order to test and ensure the company's ability to recover from a security incident.	CC7.5, CC9.1
CC.6.5.DD	The company has implemented a procedure in order to ensure that there is a process to identify data and software stored on organizational devices and dispose of this data in an appropriate manner.	CC6.5
RR.01.01	The organisation enforces and holds individual employees accountable for their internal control responsibilities, in line with their job objectives and KPIs.	CC1.5

Description of Test of Controls and Results

Security Category

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC1.1 The entity demonstrates a commitment to integrity and ethical values.			
CC.01.01	The Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	Inquired of management to determine the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control. Inspected the board meeting minutes for Calendar Q1, Q2, and Q3 of 2024 to determine that the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control.	No deviations noted.
CC.01.05	The company's employees are required to read and accept the Code of conduct, Acceptable use policy upon their hire. Management monitors employees' compliance with an official signature.	Inquired of management to determine company employees are required to read and accept a Code of conduct, and Acceptable use policy agreement prior to employment. Inspected the Code of conduct, and Acceptable use policy to determine employees are required to read and accept these policies, prior to employment.	No deviations noted.
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.01.01	The Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	Inquired of management to determine the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control. Inspected the board meeting minutes for Calendar Q1, Q2, and Q3 of 2024 to determine that the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control.	No deviations noted.
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	Inquired of management to determine that management meets on a bi-weekly basis and has a fixed agenda to oversee the company's objectives. Inspected a sample of bi-weekly management meetings and determined management meets on a bi-weekly basis to oversee the company's objectives.	No deviations noted.
CC.01.03	The company has defined structures, and reporting lines with assigned authority and responsibilities, in order to appropriately meet the security requirements.	Inquired of management to determine the company has defined structures, and reporting lines with assigned authority and responsibilities. Inspected the company organization chart to determine the company has defined structures, and reporting lines with assigned authority and responsibilities.	No deviations noted.
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	No deviations noted.
CC.01.07	The company conducts pre-employment screening checks of candidates commensurate with the employee's position and level, in accordance with local laws.	<p>Inquired of management to determine the company conducts pre-employment screening checks of candidates prior to hire, as applicable.</p> <p>Inspected the Human Resources policy to determine the company conducts pre-employment screening checks of candidates prior to hire, as applicable.</p> <p>Inspected a candidate pre-employment checklist to determine the company conducts pre-employment screening checks of candidates prior to hire, as applicable.</p> <p>Inspected the list of employees to determine there were no new hires during the attest period.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.01.08	New employees go through an onboarding process to be informed of their role responsibilities, organizational policies, and provision of relevant access.	<p>Inquired of management to determine new employees are informed of their responsibilities, organizational policies, and are provisioned access as part of the employee onboarding process.</p> <p>Inspected the Human Resources Policy to determine new employees are informed of their responsibilities, organizational policies, and are provisioned access as part of the employee onboarding process.</p> <p>Inspected the onboarding record to determine new employees are informed of their responsibilities, organizational policies, and are provisioned access as part of the employee onboarding process.</p> <p>Inspected the list of employees to determine there were no new hires during the attest period.</p>	No deviations noted.
CC.01.09	The company provides education and training to ensure that the skill sets and technical competency of employees are developed and maintained.	<p>Inquired of management to determine the company provides education and training to ensure that the skill sets and technical competency of employees are developed and maintained.</p> <p>Inspected the employee training record to determine the company provides education and training to ensure that the skill sets and technical competency of employees are developed and maintained.</p>	No deviations noted.
CC.02.02	The company has established a Security and Privacy Awareness Training program and requires all employees to complete this training every year.	<p>Inquired of management to determine employees complete the Security Awareness Training program annually.</p> <p>Inspected annual security awareness training records to determine employees complete this training annually.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.07.07	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	<p>Inquired of management to determine the company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p> <p>Inspect the incident response playbooks to determine the security incidents response playbook is maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p>	No deviations noted.
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC.01.05	The company's employees are required to read and accept the Code of conduct, Acceptable use policy upon their hire. Management monitors employees' compliance with an official signature.	<p>Inquired of management to determine company employees are required to read and accept a Code of conduct, and Acceptable use policy agreement prior to employment.</p> <p>Inspected the Code of conduct, and Acceptable use policy to determine employees are required to read and accept these policies, prior to employment.</p>	No deviations noted.
CC.01.10	The company performs an annual performance review of all employees that have been at the organization for 12 or more months. A formal evaluation of each employee is performed in alignment with the Company's objectives.	<p>Inquired of management to determine the company performs an annual performance review of all employees that have been at the organization for 12 or more months consistent with the company's objectives.</p> <p>Inspected a sample of employee performance reviews to determine an annual evaluation was completed for employees timely.</p>	No deviations noted.
RR.01.01	The organization enforces and holds individual employees accountable for their internal control responsibilities,	Inquired of management to determine organization enforces and holds individual employees accountable for their internal control responsibilities, in line with their job objectives and KPIs.	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	in line with their job objectives and KPIs.	Inspected policies and procedures to determine the company enforces and holds individual employees accountable for their internal control responsibilities, in line with their job objectives and KPIs.	
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	No deviations noted.
CC.02.01	A detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.	<p>Inquired of management to determine a detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.</p> <p>Inspected the product architecture diagram to determine a detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.</p>	No deviations noted.
CC.02.05	The company maintains external documentation describing the product features, system boundaries, user guides, and services commitments.	Inquired of management to determine the company maintains external documentation describing product features, system boundaries, user guides, and service commitments.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected the external knowledge base to determine the company maintains external documentation describing product features, system boundaries, user guides, and service commitments.	
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC.01.01	The Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	<p>Inquired of management to determine the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control.</p> <p>Inspected the board meeting minutes for Calendar Q1, Q2, and Q3 of 2024 to determine that the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control.</p>	No deviations noted.
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	<p>Inquired of management to determine that management meets on a bi-weekly basis and has a fixed agenda to oversee the company's objectives.</p> <p>Inspected a sample of bi-weekly management meetings and determined management meets on a bi-weekly basis to oversee the company's objectives.</p>	No deviations noted.
CC.01.03	The company has defined structures, and reporting lines with assigned authority and responsibilities, in order to appropriately meet the security requirements.	Inquired of management to determine the company has defined structures, and reporting lines with assigned authority and responsibilities.	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected the company organization chart to determine the company has defined structures, and reporting lines with assigned authority and responsibilities.	
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	No deviations noted.
CC.02.02	The company has established a Security and Privacy Awareness Training program and requires all employees to complete this training every year.	<p>Inquired of management to determine employees complete the Security Awareness Training program annually.</p> <p>Inspected annual security awareness training records to determine employees complete this training annually.</p>	No deviations noted.
CC.02.03	The company maintains an internal informational knowledge base describing the company's environment, its boundaries, user responsibilities and services.	<p>Inquired of management to determine the company maintains an internal informational knowledge base describing the company's environment, its boundaries, user responsibilities and services.</p> <p>Inspected the internal information knowledge base to determine it described the company's environment, its boundaries, user responsibilities, and services.</p>	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.02.04	Detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.	<p>Inquired of management to determine detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.</p> <p>Inspected the Incident Management Policy to determine detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.</p> <p>Inspected configurations of the tools used to monitor security systems to determine it is set up to identify and detect security events that are not reported by a user.</p>	No deviations noted.
CC.02.07	Release notes are sent internally describing the closed stories that were part of new versions released on a bi-weekly basis.	<p>Inquired of management to determine release notes are sent internally to personnel upon new product releases.</p> <p>Inspected a sample of product releases to determine release notes are sent bi-weekly internally to personnel upon new product releases.</p>	No deviations noted.
CC.07.07	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	<p>Inquired of management to determine the company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p> <p>Inspect the incident response playbooks to determine the security incidents response playbook is maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p>	No deviations noted.
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.			



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.01.01	The Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	<p>Inquired of management to determine the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control.</p> <p>Inspected the board meeting minutes for Calendar Q1, Q2, and Q3 of 2024 to determine that the Board of Directors meets quarterly, demonstrates independence from management, and exercises oversight over the development and performance of internal control.</p>	No deviations noted.
CC.02.05	The company maintains external documentation describing the product features, system boundaries, user guides, and services commitments.	<p>Inquired of management to determine the company maintains external documentation describing product features, system boundaries, user guides, and service commitments.</p> <p>Inspected the external knowledge base to determine the company maintains external documentation describing product features, system boundaries, user guides, and service commitments.</p>	No deviations noted.
CC.02.06	New features are communicated to customers through email to keep them updated on new product features on a quarterly basis.	<p>Inquired of management to determine new features are communicated to customers through the company newsletter to keep them updated on new product features upon release on a quarterly basis .</p> <p>Inspected a sample product release notes to determine new features are communicated to customers through the company newsletter to keep them updated on new product features upon release on a quarterly basis.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.02.08	Customers are notified of service interruptions through email.	<p>Inquired of management to determine customers are notified of service interruptions through the company's website.</p> <p>Inspected uptime application status records, to determine no service interruptions occurred within the attestation period.</p> <p>Inspected the service interruption communications process to determine one exists for the company to follow in the event of client service interruptions.</p>	No deviations noted.
CC.02.09	Client issues are reported to the company via a dedicated support email address. Support issues are handled by using a ticketing system.	<p>Inquired of management to determine customer issues are reported to the company via a dedicated email address and that support issues are handled using a ticketing system.</p> <p>Inspected the company's email address to determine client issues are reported via the email address and support issues are handled using a ticketing system</p>	No deviations noted.
CC.02.11	Customers/Users are provided with communication channels to report failures, incidents, and other complaints to the company.	<p>Inquired of management to determine customers/users are provided with communication channels on the website to report failures, incidents, and other complaints to the company.</p> <p>Inspected communication channels to determine customers/users are provided with channels to report failures, incidents, and other complaints</p>	No deviations noted.
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.03.01	The company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.	<p>Inquired of management to determine the company maintains a formal risk management program.</p> <p>Inspected the Risk Assessment and Treatment Policy to determine the company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the company's risk assessment to determine the assessment was performed annually.</p>	No deviations noted.
CC.03.03	The annual risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	<p>Inquired of management to determine that senior management review the annual risk assessment on an annual basis and minutes of the meeting and action items are documented.</p> <p>Inspected the risk assessment and meeting minutes to determine the risk assessment was reviewed annually and action items were reviewed and approved.</p>	No deviations noted.
CC3.2 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.			
CC.03.01	The company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options	<p>Inquired of management to determine the company maintains a formal risk management program.</p> <p>Inspected the Risk Assessment and Treatment Policy to determine the company maintains a formal risk management program to assess information security risks that impact the company's business</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	may include acceptance, avoidance, mitigation, and transfer.	objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.	
		Inspected the company's risk assessment to determine the assessment was performed annually.	
CC.03.03	The annual risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	Inquired of management to determine that senior management review the annual risk assessment on an annual basis and minutes of the meeting and action items are documented. Inspected the risk assessment and meeting minutes to determine the risk assessment was reviewed annually and action items were reviewed and approved.	No deviations noted.
CC.03.04	The company identifies, classifies and manages the inventory of information assets. The assets inventory is reviewed by the CTO on an annual basis.	Inquired of management to determine the company identifies, classifies, and manages an inventory of information assets that is reviewed by the CTO on an annual basis. Inspected the inventory of information assets to determine it was reviewed by the CTO on an annual basis.	No deviations noted.
CC.09.02	The company assesses, on an annual basis, the risks that vendors and business partners represent to the achievement of the Company's objectives.	Inquired of management to determine the company assesses vendor risks to achievement of company objectives on an annual basis. Inspected the third party risk assessment to determine the company assesses vendor risks to achievement of company objectives on an annual basis.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.09.04	The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	Inquired of management to determine the company reviews the critical vendors' SOC 2 report on an annual basis, including identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion. Inspected the annual vendor security review to determine the company reviews the critical vendors' SOC 2 report on an annual basis, including identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	No deviations noted.
CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC.03.01	The company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.	Inquired of management to determine the company maintains a formal risk management program. Inspected the Risk Assessment and Treatment Policy to determine the company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. Inspected the company's risk assessment to determine the assessment was performed annually.	No deviations noted.
CC.03.03	The annual risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	Inquired of management to determine that senior management review the annual risk assessment on an annual basis and minutes of the meeting and action items are documented.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected the risk assessment and meeting minutes to determine the risk assessment was reviewed annually and action items were reviewed and approved.	
CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC.03.01	The company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.	<p>Inquired of management to determine the company maintains a formal risk management program.</p> <p>Inspected the Risk Assessment and Treatment Policy to determine the company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the company's risk assessment to determine the assessment was performed annually.</p>	No deviations noted.
CC.03.03	The annual risk assessment summary is presented to senior management for review, comment, and approval. Minutes of the meeting and action items are documented.	<p>Inquired of management to determine that senior management review the annual risk assessment on an annual basis and minutes of the meeting and action items are documented.</p> <p>Inspected the risk assessment and meeting minutes to determine the risk assessment was reviewed annually and action items were reviewed and approved.</p>	No deviations noted.
CC.07.07	The company's contingency planning and incident response playbooks are maintained and updated to reflect	Inquired of management to determine the company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	emerging continuity risks and lessons learned from past incidents.	Inspect the incident response playbooks to determine the security incidents response playbook is maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	
CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	Inquired of management to determine that management meets on a bi-weekly basis and has a fixed agenda to oversee the company's objectives. Inspected a sample of bi-weekly management meetings and determined management meets on a bi-weekly basis to oversee the company's objectives.	No deviations noted.
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees. Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	No deviations noted.
CC.04.01	An external web application penetration test is conducted annually. Critical and High issues are	Inquired of management to determine an external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	investigated and resolved in a timely manner.	Inspected the annual penetration test report to determine an external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.	
CC4.2 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.			
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	<p>Inquired of management to determine that management meets on a bi-weekly basis and has a fixed agenda to oversee the company's objectives.</p> <p>Inspected a sample of bi-weekly management meetings and determined management meets on a bi-weekly basis to oversee the company's objectives.</p>	No deviations noted.
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	No deviations noted.
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	<p>Inquired of management to determine that management meets on a bi-weekly basis and has a fixed agenda to oversee the company's objectives.</p> <p>Inspected a sample of bi-weekly management meetings and determined management meets on a bi-weekly basis to oversee the company's objectives.</p>	No deviations noted.
CC.03.01	The company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.	<p>Inquired of management to determine the company maintains a formal risk management program.</p> <p>Inspected the Risk Assessment and Treatment Policy to determine the company maintains a formal risk management program to assess information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.</p> <p>Inspected the company's risk assessment to determine the assessment was performed annually.</p>	No deviations noted.
CC.05.02	Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.	<p>Inquired of management to determine developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.</p> <p>Inspected access to the production environment to determine developers have limited access to production environment resources and that developers have read-only production access to all production buckets.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected population of privilege escalation process to determine developers do not have access to the production environments, and can be granted temporary access after getting approval.	
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC.01.02	The Management of the company meets on a bi-weekly basis, and has a fixed agenda to oversee the company's objectives.	<p>Inquired of management to determine that management meets on a bi-weekly basis and has a fixed agenda to oversee the company's objectives.</p> <p>Inspected a sample of bi-weekly management meetings and determined management meets on a bi-weekly basis to oversee the company's objectives.</p>	No deviations noted.
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	No deviations noted.
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the	Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	management, and are available to the company's employees.	Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	
CC.07.07	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	<p>Inquired of management to determine the company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p> <p>Inspect the incident response playbooks to determine the security incidents response playbook is maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p>	No deviations noted.
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC.02.01	A detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.	<p>Inquired of management to determine a detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.</p> <p>Inspected the product architecture diagram to determine a detailed description of the product architecture and system boundaries is documented and available internally to the company's employees.</p>	No deviations noted.
CC.03.04	The company identifies, classifies and manages the inventory of information assets. The assets inventory is	Inquired of management to determine the company identifies, classifies, and manages an inventory of information assets that is reviewed by the CTO on an annual basis.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	reviewed by the CTO on an annual basis.	Inspected the inventory of information assets to determine it was reviewed by the CTO on an annual basis.	
CC.05.02	Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.	<p>Inquired of management to determine developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.</p> <p>Inspected access to the production environment to determine developers have limited access to production environment resources and that developers have read-only production access to all production buckets.</p> <p>Inspected population of privilege escalation process to determine developers do not have access to the production environments, and can be granted temporary access after getting approval.</p>	No deviations noted.
CC.06.01	All access requests to organizational systems, including administrator accounts, are approved prior to access provisioning.	<p>Inquired of management to determine access requests are reviewed and approved prior to provisioning.</p> <p>Inspected the population of access request records to determine access requests are reviewed and approved prior to provisioning.</p>	No deviations noted.
CC.06.02	The company manages access governance through a roles-based access control matrix based on the job description and responsibilities.	<p>Inquired of management to determine access is managed through a role-based access model.</p> <p>Inspected the access control matrix to determine access is managed through a role-based access model.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.06.03	<p>The company has established a formal standard for passwords to govern the management and use of authentication mechanisms. Strong password configuration settings, where applicable, are enabled, including:</p> <ul style="list-style-type: none"> (1) Use a minimum of 8 characters (2) Use upper case, lower case, numeric, and special character values 	<p>Inquired of management to determine the company has established a formal standard for passwords to govern the management and use of authentication mechanisms.</p> <p>Inspected the Access Control Policy to determine the company has established a formal standard for passwords to govern the management and use of authentication mechanisms.</p> <p>Inspected the password policy configuration to determine the company enforces authentication requirements including:</p> <ul style="list-style-type: none"> (1) Use a minimum of 8 characters (2) Use upper case, lower case, numeric, and special character values 	No deviations noted.
CC.06.05	Access to the identity management tool is performed using two-factor authentication and is restricted to authorized personnel.	<p>Inquired of management to determine access to the identity management tool requires two-factor authentication and is restricted to authorized personnel.</p> <p>Inspected the list of users with privileged access to the identity management tool to determine access is restricted to authorized personnel.</p> <p>Inspected the identity management tool authentication configuration to determine access to the identity management tool requires two-factor authentication.</p> <p>Inspected the IAM tool to determine applications that use SSO (Single Sign On) to authenticate users are integrated with the tool.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.06.06	Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method.	<p>Inquired of management to determine access to the production environment console requires two-factor authentication and is restricted to authorized personnel.</p> <p>Inspected the list of users with privileged access to the production environment console to determine access is restricted to authorized personnel.</p> <p>Inspected the production environment console authentication configuration to determine access requires two-factor authentication.</p>	No deviations noted.
CC.06.08	Access to sensitive databases is restricted to authorized users and uses a VPN.	<p>Inquired of management to determine access to sensitive databases requires two-factor authentication and is restricted to authorized personnel.</p> <p>Inspected the list of users with access to sensitive databases to determine access to sensitive databases is restricted to authorized personnel.</p> <p>Inspected the sensitive database authentication configuration to determine access to sensitive databases requires VPN access</p>	No deviations noted.
CC.06.09	Access to the source control tool is performed using two-factor authentication and is restricted to authorized personnel.	Inquired of management to determine access to the source control tool requires two-factor authentication and is restricted to authorized personnel.	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		<p>Inspected the list of users with access to the source control tool to determine access to the source control tool is restricted to authorized personnel.</p> <p>Inspected the source control tool authentication configuration to determine access to the source control tool requires two-factor authentication.</p>	
CC.06.10	The access to the production server is performed using the two-factor authentication method.	<p>Inquired of management to determine access to the production server requires two-factor authentication and is restricted to authorized personnel.</p> <p>Inspected the list of users with access to the production server to determine access to the production server is restricted to authorized personnel.</p> <p>Inspected the production server authentication configuration to determine access to the production server requires two-factor authentication.</p>	No deviations noted.
CC.06.11	Access to alter and delete backups is restricted to authorized users and performed using a two-factor authentication.	<p>Inquired of management to determine access to alter and delete backups requires two-factor authentication and is restricted to authorized users.</p> <p>Inspected the cloud production environment to determine access to alter and delete backups is restricted to authorized users.</p>	No deviations noted.

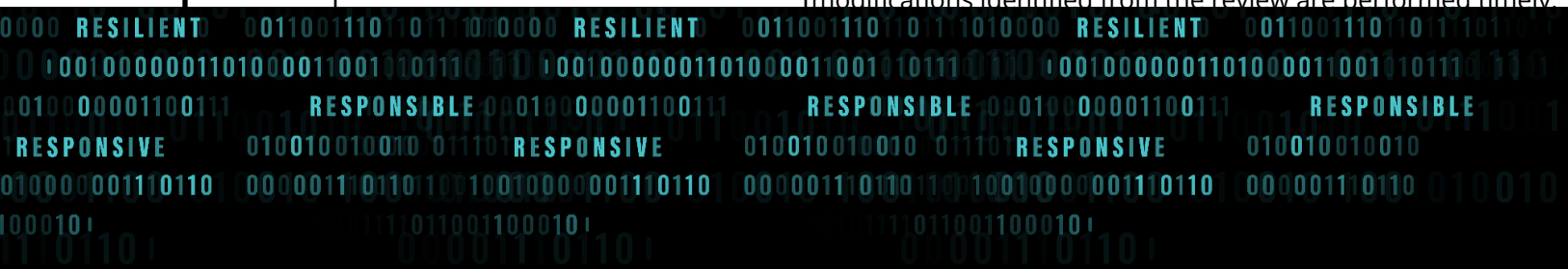
Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected the cloud production environment authentication configuration to determine access to alter and delete backups requires two-factor authentication.	
CC.06.13	The company has an established key management process in place to support the organization's use of cryptographic techniques.	<p>Inquired of management to determine the company has an established key management process in place to support the organization's use of cryptographic techniques.</p> <p>Inspected a sample of customer managed encryption keys to determine the company utilizes Amazon AWS Key Management System (KMS) to support the organization's use of cryptographic techniques, including use of 256-bit encryption algorithms, and hardware security modules (HSM) managed by Amazon.</p>	No deviations noted.
CC.06.14	Provisioning of new user access must follow a notification from HR.	<p>Inquired of management to determine new user access is provisioned upon confirmation of employment date and role from HR personnel.</p> <p>Inspected the Access Control Policy to determine new user access is provisioned upon confirmation of employment date and role from HR personnel.</p> <p>Inspected the list of employees to determine there were no new hires during the attestation period.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.06.24	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	<p>Inquired of management to determine information assets containing sensitive customer data are at least disk-level encrypted.</p> <p>Inspected the Encryption Key Management Policy to determine information assets containing sensitive customer data are at least disk-level encrypted.</p> <p>Inspected encryption configurations of information assets to determine information assets containing sensitive customer data are disk-level encrypted.</p>	No deviations noted.
CC.06.25	The company secures and controls its employees' devices to enforce security settings including - hard-disk encryption, auto patching, password requirement, auto screen-lock, remote wipe capabilities, antivirus and deployment of additional policies.	<p>Inquired of management to determine the company enforces hard-disk encryption, auto patching, password requirement, and auto screen-lock and remote wipe capabilities.</p> <p>Inspected employee device management configurations to determine the company enforces hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities on employee end-user devices.</p>	No deviations noted.
CC.08.11	The company enforced segregation between development, staging, and production environments to enforce confidentiality and privacy of customers' data.	<p>Inquired of management to determine the company segregates development, staging, and production environments.</p> <p>Inspected cloud architecture to determine the company segregates development, staging, and production environments.</p>	No deviations noted.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	accounts, are approved prior to access provisioning.	Inspected the population of access request records to determine access requests are reviewed and approved prior to provisioning.	
CC.06.02	The company manages access governance through a roles-based access control matrix based on the job description and responsibilities.	<p>Inquired of management to determine access is managed through a role-based access model.</p> <p>Inspected the access control matrix to determine access is managed through a role-based access model.</p>	No deviations noted.
CC.06.16	User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination. Additionally, upon leaving, organizational assets shall be returned.	<p>Inquired of management to determine user access is revoked timely upon notification of employee termination.</p> <p>Inspected the off-boarding checklist to determine a formal process is implemented to ensure user accounts are disabled or deleted on the production and other organizational information assets timely.</p> <p>Inspected the list of terminated users to determine no personnel left the company during the attestation period.</p>	No deviations noted.
CC.06.17	User access and permissions are reviewed and approved by the company's management on a quarterly basis.	<p>Inquired of management to determine user access is reviewed and approved on a quarterly basis.</p> <p>Inspected a sample of user access reviews to determine privileges are reviewed on a quarterly basis and necessary access modifications identified from the review are performed timely.</p>	No deviations noted.

enter facilities,

S.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.06.20	Physical access to the offices is restricted to authorized personnel RFID key fobs. The Key Fob is needed within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	<p>Inquired of management to determine physical access to the offices is restricted to authorized personnel with RFID key fob. The key fob is needed within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.</p> <p>Inspected the Physical Security Policy to determine the company maintains physical restriction requirements for sensitive facilities.</p> <p>Inspected the access list for the office to determine offices are restricted to authorized personnel with RFID key fob. The key fob is needed within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.</p>	No deviations noted.
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.			
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC.06.16	User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination. Additionally, upon leaving, organizational assets shall be returned.	<p>Inquired of management to determine user access is revoked timely upon notification of employee termination.</p> <p>Inspected the off-boarding checklist to determine a formal process is implemented to ensure user accounts are disabled or deleted on the production and other organizational information assets timely.</p> <p>Inspected the list of terminated users to determine no personnel left the company during the attestation period.</p>	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.6.5.DD	The company has implemented a procedure in order to ensure that there is a process to identify data and software stored on organizational devices and dispose of this data in an appropriate manner.	Inquired of management to determine the company has implemented a procedure in order to ensure that there is a process to identify data and software stored on organizational devices and dispose of this data in an appropriate manner. Inspected the Record Retention Policy to determine the company has procedures in place to identify data and software stored on organizational devices and dispose of this data in an appropriate manner.	No deviations noted.
<p>AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting where the services reside.</p> <p>AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.</p>			
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC.06.21	The company has enabled multiple network security controls such as SSH restriction, and port restriction	Inquired of management to determine the company configures security rules such as SSH restriction, and port restriction. Inspected the configured security rules for SSH restriction and port restriction to determine the company configures security rules to filter unauthorized network traffic.	No deviations noted.
CC.06.22	The company has enforced a strict policy for the protection of customer passwords through hashing.	Inquired of management to determine the company has enforced strict policy for the protection of customer passwords through hashing.	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected the client's password management system to determine that customers' passwords are hashed within the company's user database.	
CC.06.23	Encrypted communication between the company's customers and the company's assets is enabled using at least a valid HTTPS TLS 1.2 authenticated certificate.	<p>Inquired of management to determine communication between the company's customers and the company's assets is encrypted via TLS 1.2 protocol.</p> <p>Inspected the company's web application domain configuration to determine transmissions between the company's customers and the company's assets to enforce TLS 1.2 encryption protocol.</p> <p>Inspected the connection settings to the organization's external websites for a user to determine encrypted communication between the company's customers and the company's assets is enabled using a valid HTTPS TLS 1.2 authenticated certificate.</p>	No deviations noted.
CC.06.24	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	<p>Inquired of management to determine information assets containing sensitive customer data are at least disk-level encrypted.</p> <p>Inspected the Encryption Key Management Policy to determine information assets containing sensitive customer data are at least disk-level encrypted.</p> <p>Inspected encryption configurations of information assets to determine information assets containing sensitive customer data are disk-level encrypted.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC.06.22	The company has enforced a strict policy for the protection of customer passwords through hashing.	<p>Inquired of management to determine the company has enforced strict policy for the protection of customer passwords through hashing.</p> <p>Inspected the client's password management system to determine that customers' passwords are hashed within the company's user database.</p>	No deviations noted.
CC.06.23	Encrypted communication between the company's customers and the company's assets is enabled using at least a valid HTTPS TLS 1.2 authenticated certificate.	<p>Inquired of management to determine communication between the company's customers and the company's assets is encrypted via TLS 1.2 protocol.</p> <p>Inspected the company's web application domain configuration to determine transmissions between the company's customers and the company's assets to enforce the TLS 1.2 encryption protocol.</p> <p>Inspected the connection settings to the organization's external websites for a user to determine encrypted communication between the company's customers and the company's assets is enabled using a valid HTTPS TLS 1.2 authenticated certificate.</p>	No deviations noted.
CC.06.24	Restricted information assets containing sensitive customer data hosted on databases, storage, and backups are at least disk-level encrypted.	<p>Inquired of management to determine information assets containing sensitive customer data are at least disk-level encrypted.</p> <p>Inspected the Encryption Key Management Policy to determine information assets containing sensitive customer data are at least disk-level encrypted.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected encryption configurations of information assets to determine information assets containing sensitive customer data are disk-level encrypted.	
CC.06.25	The company secures and controls its employees' devices to enforce security settings including - hard-disk encryption, auto patching, password requirement, auto screen-lock, remote wipe capabilities, antivirus and deployment of additional policies.	<p>Inquired of management to determine the company enforces hard-disk encryption, auto patching, password requirement, and auto screen-lock and remote wipe capabilities.</p> <p>Inspected employee device management configurations to determine the company enforces hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities on employee end-user devices.</p>	No deviations noted.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC.01.04	Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	No deviations noted.
CC.06.25	The company secures and controls its employees' devices to enforce security settings including - hard-disk	Inquired of management to determine the company enforces hard-disk encryption, auto patching, password requirement, and auto screen-lock and remote wipe capabilities.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	encryption, auto patching, password requirement, auto screen-lock, remote wipe capabilities, antivirus and deployment of additional policies.	Inspected employee device management configurations to determine the company enforces hard-disk encryption, auto patching, password requirement, auto screen-lock, and remote wipe capabilities on employee end-user devices.	
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC.04.01	An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.	<p>Inquired of management to determine an external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner</p> <p>Inspected the annual penetration test report to determine an external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.</p>	No deviations noted.
CC.07.01	Production networks undergo vulnerability scans continuously. A quarterly review is performed and critical/high issues identified are tracked and remediated in accordance with the Vulnerability and Threat Management Policy.	<p>Inquired of management to determine production networks undergo vulnerability scans on a quarterly basis. Detected incidents are investigated and resolved in accordance with the Vulnerability and Threat Management Policy.</p> <p>Inspected the Vulnerability and Threat Management Policy to determine production networks undergo vulnerability scans on a quarterly basis and detected incidents are investigated and resolved in accordance to the Vulnerability and Threat Management Policy.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected a sample of vulnerability reviews to determine vulnerabilities are detected, investigated and resolved in accordance with the Vulnerability and Threat Management Policy.	
CC.08.05	Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated.	<p>Inquired of management to determine source code vulnerability scans are performed and identified issues are remediated per resolution policy.</p> <p>Inspected the Threat and Vulnerability Management policy to determine source code vulnerability scans are performed and identified issues are remediated per the policy.</p> <p>Inspected the source code vulnerability scanner to determine source code vulnerability scans are performed and identified issues are remediated per resolution policy.</p> <p>Inspected a sample high or critical severity vulnerabilities to determine issues are remediated timely.</p>	No deviations noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC.04.01	An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.	<p>Inquired of management to determine an external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner</p> <p>Inspected the annual penetration test report to determine an external web application penetration test is conducted annually.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Critical and High issues are investigated and resolved in a timely manner.	
CC.07.02	Audit trail (security logs) is deployed on the production environment continuously to capture actions made directly by the user or a cloud service.	Inquired of management to determine continuous audit logging is enabled across the production environment. Inspected audit log configurations to determine audit logging is enabled across the production environment.	No deviations noted.
CC.07.03	Audit trail security logs are configured to be retained for 365 days.	Inquired of management to determine audit trail security logs are configured to be retained for 365 days. Inspected audit trail configurations to determine audit trail security logs are configured to be retained for 365 days.	No deviations noted.
CC.07.04	Intrusion detection system scans continuously for potential security issues and alerts the administrator upon discovering unexpected and potentially malicious activity in the production environment, with a high/critical risk rating. A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring.	Inquired of management to determine an intrusion detection system and incident ticketing system are implemented to identify and track the occurrence and severity of incidents. Inspected the cloud production environment to determine an intrusion detection system and incident ticketing system are implemented to identify and track the occurrence and severity of incidents. Inspected Intrusion detection findings and incident tickets to determine identified incidents are tracked to resolution consistent with the company's Incident Management policy.	No deviations noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.02.04	Detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.	<p>Inquired of management to determine detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.</p> <p>Inspected the Incident Management Policy to determine detected incidents are communicated and reviewed by the individual responsible for the management of the security in the company.</p> <p>Inspected configurations of the tools used to monitor security systems to determine it is set up to identify and detect security events that are not reported by a user.</p>	No deviations noted.
CC.07.04	Intrusion detection system scans continuously for potential security issues and alerts the administrator upon discovering unexpected and potentially malicious activity in the production environment, with a high/critical risk rating. A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effectiveness monitoring.	<p>Inquired of management to determine an intrusion detection system and incident ticketing system are implemented to identify and track the occurrence and severity of incidents.</p> <p>Inspected the cloud production environment to determine an intrusion detection system and incident ticketing system are implemented to identify and track the occurrence and severity of incidents.</p> <p>Inspected Intrusion detection findings and incident tickets to determine identified incidents are tracked to resolution consistent with the company's Incident Management policy.</p>	No deviations noted.
CC.07.06	The company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in	Inquired of management to determine the company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
	accordance with applicable laws and regulations.	Inspected the Security Incident Response Policy to determine measures are in place to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	
CC.07.07	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	<p>Inquired of management to determine the company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p> <p>Inspect the incident response playbooks to determine the security incidents response playbook is maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.</p>	No deviations noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC.02.08	Customers are notified of service interruptions through email.	<p>Inquired of management to determine customers are notified of service interruptions through the company's website.</p> <p>Inspected uptime application status records, to determine no service interruptions occurred within the attestation period.</p> <p>Inspected the service interruption communications process to determine one exists for the company to follow in the event of client service interruptions.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
CC.07.01	Production networks undergo vulnerability scans continuously. A quarterly review is performed and critical/high issues identified are tracked and remediated in accordance with the Vulnerability and Threat Management Policy.	<p>Inquired of management to determine production networks undergo vulnerability scans on a quarterly basis. Detected incidents are investigated and resolved in accordance with the Vulnerability and Threat Management Policy.</p> <p>Inspected the Vulnerability and Threat Management Policy to determine production networks undergo vulnerability scans on a quarterly basis and detected incidents are investigated and resolved in accordance to the Vulnerability and Threat Management Policy.</p> <p>Inspected a sample of vulnerability reviews to determine vulnerabilities are detected, investigated and resolved in accordance with the Vulnerability and Threat Management Policy.</p>	No deviations noted.
CC.07.06	The company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	<p>Inquired of management to determine the company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.</p> <p>Inspected the Security Incident Response Policy to determine measures are in place to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.</p>	No deviations noted.
CC.07.07	The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	Inquired of management to determine the company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspect the incident response playbooks to determine the security incidents response playbook is maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.	
CC.07.08	A root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution.	<p>Inquired of management to determine that a root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution.</p> <p>Inspected the root cause analysis procedure document to determine that a process has been defined to document root causes of security incidents to prepare change requests for initiating the remediation process.</p>	No deviations noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC.02.08	Customers are notified of service interruptions through email.	<p>Inquired of management to determine customers are notified of service interruptions through the company's website.</p> <p>Inspected uptime application status records, to determine no service interruptions occurred within the attestation period.</p> <p>Inspected the service interruption communications process to determine one exists for the company to follow in the event of client service interruptions.</p>	No deviations noted.



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results
CC.07.06	The company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.	<p>Inquired of management to determine the company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.</p> <p>Inspected the Security Incident Response Policy to determine measures are in place to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.</p>
CC.07.08	A root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution.	<p>Inquired of management to determine that a root cause analysis is prepared and reviewed by management for high severity incidents. Change requests are prepared based on the root cause analysis to remediation and resolution.</p> <p>Inspected the root cause analysis procedure document to determine that a process has been defined to document root causes of security incidents to prepare change requests for initiating the remediation process.</p>
AV.03.02	Data restoration checks are performed continuously in order to test and ensure the company's ability to recover from a security incident.	<p>Inquired of management to determine data restoration checks are performed continuously in order to test and ensure the company's ability to recover from a security incident.</p> <p>Inspected the data restoration check procedure to determine it is performed continuously and ensures the company's ability to recover from a security incident.</p>

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		<p>Inspected the data restoration check script to determine it is configured to execute as part of the company's automated testing as part of the SDLC.</p> <p>Inspected a sample automated test execution to determine data restoration checks are performed continuously.</p>	
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC.01.04	<p>Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	<p>Inquired of management to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p> <p>Inspected the company policies and procedures to determine formal policies and procedures are documented, reviewed, and approved on an annual basis by the management, and are available to the company's employees.</p>	<p>No deviations noted.</p>
CC.05.02	<p>Developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.</p>	<p>Inquired of management to determine developers do not have access to the production environments. For emergency purposes, temporary access can be granted after getting approval.</p> <p>Inspected access to the production environment to determine developers have limited access to production environment resources and that developers have read-only production access to all production buckets.</p>	<p>No deviations noted.</p>



Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		Inspected population of privilege escalation process to determine developers do not have access to the production environments, and can be granted temporary access after getting approval.	
CC.08.01	Request tickets are created to document change requests within the change management system. Pull requests and change tickets are linked to each other so the code change can be tracked.	<p>Inquired of management to determine code pull requests and corresponding production code change requests are tracked within the change management system.</p> <p>Inspected the change management system to determine code pull requests and corresponding production code change requests are tracked within the change management system.</p>	No deviations noted.
CC.08.04	Code changes must be reviewed and approved in order to progress through the SDLC and deploy a version to production.	<p>Inquired of management to determine code changes must be reviewed and approved prior to deployment into production.</p> <p>Inspected the change management system configuration to determine code changes must be reviewed and approved by an individual over than the change developer prior to deployment into production.</p>	No deviations noted.
CC.08.05	Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated.	<p>Inquired of management to determine source code vulnerability scans are performed and identified issues are remediated per resolution policy.</p> <p>Inspected the Threat and Vulnerability Management policy to determine source code vulnerability scans are performed and identified issues are remediated per the policy.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
		<p>Inspected the source code vulnerability scanner to determine source code vulnerability scans are performed and identified issues are remediated per resolution policy.</p> <p>Inspected a sample high or critical severity vulnerabilities to determine issues are remediated timely.</p>	
CC.08.07	A successful test result is mandatory in order to continue with the SDLC process and deploy a version to the production environment. In cases of test failures, the build is stopped and does not deploy.	<p>Inquired of management to determine changes to production source code are tested prior to deployment.</p> <p>Inspected the change management system configuration to determine changes to production source code are tested prior to deployment.</p>	No deviations noted
CC.08.08	The company developed a process in order to manage emergency changes. A post approval process is performed for each emergency change.	<p>Inquired of management to determine retroactive approvals are obtained for emergency changes.</p> <p>Inspected the SDLC Policy for emergency change process to determine retroactive approvals are obtained for emergency changes.</p> <p>Inspected the change management logs to determine there were no emergency changes that occurred during the attestation period.</p>	No deviations noted.
CC.08.11	The company enforced segregation between development, staging, and production environments to enforce confidentiality and privacy of customers' data.	<p>Inquired of management to determine the company segregates development, staging, and production environments.</p> <p>Inspected cloud architecture to determine the company segregates development, staging, and production environments.</p>	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results	
AV.03.02	Data restoration checks are performed continuously in order to test and ensure the company's ability to recover from a security incident.	<p>Inquired of management to determine data restoration checks are performed continuously in order to test and ensure the company's ability to recover from a security incident.</p> <p>Inspected the data restoration check procedure to determine it is performed continuously and ensures the company's ability to recover from a security incident.</p> <p>Inspected the data restoration check script to determine it is configured to execute as part of the company's automated testing as part of the SDLC.</p> <p>Inspected a sample automated test execution to determine data restoration checks are performed continuously.</p>	No deviations noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC.09.02	The company assesses, on an annual basis, the risks that vendors and business partners represent to the achievement of the Company's objectives.	<p>Inquired of management to determine the company assesses vendor risks to achievement of company objectives on an annual basis.</p> <p>Inspected the third party risk assessment to determine the company assesses vendor risks to achievement of company objectives on an annual basis.</p>	No deviations noted.
CC.09.04	The company reviews the critical vendors' SOC2 report on an annual basis. The review includes identifying and documenting the controls in place at the company to address the	Inquired of management to determine the company reviews the critical vendors' SOC 2 report on an annual basis, including identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.	No deviations noted.

Control #	Controls Specified by SMT Data	Tests Performed by Decrypt Compliance PC and Test Results
	CUECs, noted deviations, and the auditor's opinion.	Inspected the annual vendor security review to determine the company reviews the critical vendors' SOC 2 report on an annual basis, including identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.

0000 RESILIENT 0011001110110100000 RESILIENT 001100111011010000 RESILIENT 001100111011010000 RESILIENT
00010000001101000011001101110110000100000011010000110011011101110
0010000001100111 RESPONSIBLE 0001000001100111 RESPONSIBLE 0001000001100111 RESPONSIBLE
RESPONSIVE 010010010010 011101 RESPONSIVE 010010010010 011101 RESPONSIVE 010010010010
01000000110110 0000011011011011001000000110110 000001101101101100100000110110 00000110110 010010
100010 1111011001100010 1111011001100010 1111011001100010
1110110 0000110110 0000110110

0000 RESILIENT 001100111011010000 RESILIENT 001100111011010000 RESILIENT 001100111011010000 RESILIENT
00010000001101000011001101110110000100000011010000110011011101110
0010000001100111 RESPONSIBLE 0001000001100111 RESPONSIBLE 0001000001100111 RESPONSIBLE
RESPONSIVE 010010010010 011101 RESPONSIVE 010010010010 011101 RESPONSIVE 010010010010
00100000110110 000001101101101100100000110110 000001101101101100100000110110 00000110110 010010
100010 1111011001100010 1111011001100010 1111011001100010
1110110 0000110110 0000110110

DECRYPT
U R L f o r e

COMPLIANCE