SOC 2 Type II Report

For the Period July 1, 2024 to June 30, 2025

REPORT ON CONTROLS PLACED IN OPERATION AT TRUSTMI NETWORK LTD. RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY AND PRIVACY WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT INCLUDING TESTS PERFORMED AND RESULTS THEREOF.

Table of Contents

Section I – Trustmi Network Ltd.’s Management Assertion

July 31, 2025

We have prepared the accompanying "Description of the Trustmi Platform relevant to Security, Availability, Confidentiality and Privacy throughout the period July 01, 2024 to June 30, 2025" (Description) of Trustmi Network Ltd. (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 Trustmi Platform (System) that may be useful when assessing the risks arising from interactions with the System , 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 relevant to Security, Availability, Confidentiality and Privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Carved-out Unaffiliated Subservice Organization: Trustmi Network Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The Description indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Trustmi Network Ltd. to achieve the service commitments and system requirements. The Description presents Trustmi Network Ltd.’s controls and the types of complementary subservice organization controls assumed in the design of Trustmi Network Ltd.’s controls. The Description does not disclose the actual controls at the carved-out AWS.

Complementary user entity controls: The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Trustmi Network Ltd.’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

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 01, 2024 to June 30, 2025 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period July 01, 2024 to June 30, 2025 to provide reasonable assurance that Trustmi Network Ltd. service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and if the carved-out subservice organization applied the controls assumed in the design of Trustmi Network Ltd.’s controls throughout that period.

c. The Trustmi Network Ltd. controls stated in the Description operated effectively throughout the period July 01, 2024 to June 30, 2025 to provide reasonable assurance that Trustmi Network Ltd.’s service commitments and system requirements were achieved based on the applicable trust services criteria, if the carved-out subservice organization applied the controls assumed in the design of Trustmi Network Ltd.’s controls throughout that period.

Eli Ben Nun
Trustmi CTO

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Section II – Independent service auditor's report

To the Management of Trustmi Network Ltd.

Scope

We have examined Trustmi Network Ltd.'s accompanying description titled "Description of the Trustmi Platform relevant to Security, Availability, Confidentiality and Privacy throughout the period July 01, 2024 to June 30, 2025" (Description) 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) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period July 01, 2024 to June 30, 2025 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA Trust Services Criteria.

Carved-out Unaffiliated Subservice Organization: Trustmi Network Ltd. uses Amazon Web Services ('AWS') (subservice organization) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Trustmi Network Ltd., to provide reasonable assurance that Trustmi Network Ltd.'s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents Trustmi Network Ltd.'s system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and are operating effectively at AWS. The Description does not disclose the actual controls at AWS. Our examination did not include the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period July 01, 2024 to June 30, 2025.

Complementary user entity controls: The Description indicates that Trustmi Network Ltd.'s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Trustmi Network Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Trustmi Network Ltd.'s responsibilities

Trustmi Network Ltd. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. Trustmi Network Ltd. has provided the accompanying assertion titled, Trustmi Network Ltd.'s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Trustmi Network Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated therein to achieve the service organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period July 01, 2024 to June 30, 2025. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Our examination was not conducted for the purpose of evaluating the performance or integrity of Trustmi Network Ltd.'s AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Trustmi Network Ltd.'s AI services.

We are required to be independent of Trustmi Network Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any

evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. the Description presents the Trustmi Platform system that was designed and implemented throughout the period July 01, 2024 to June 30, 2025 in accordance with the Description Criteria.
b. the controls stated in the Description were suitably designed throughout the period July 01, 2024 to June 30, 2025, to provide reasonable assurance that Trustmi Network Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Trustmi Network Ltd.'s controls throughout that period.
c. the controls stated in the Description operated effectively throughout the period July 01, 2024 to June 30, 2025 to provide reasonable assurance that Trustmi Network Ltd. service commitments and system requirements were achieved based on the applicable trust services criteria if the complementary subservice organization and user entity controls assumed in the design of Trustmi Network Ltd.'s controls operated effectively throughout that period.

Restricted use

This report , including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Trustmi Network Ltd., user entities of Trustmi Network Ltd.'s Trustmi Platform system during some or all of the period July 01, 2024 to June 30, 2025 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they interact with related controls at the service organization.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global

Kost Forer Gabbay and Kasierer

July 31, 2025
Tel-Aviv, Israel

Section III – Description of the Trustmi Platform relevant to Security, Availability, Confidentiality and Privacy throughout the period July 01, 2024 to June 30, 2025

Purpose and scope of the report

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

Note: *Parenthetical references have been included in the following narrative as a cross-reference to the applicable control procedures included in the Description of Criteria, Controls, Tests and Results of Tests section of this report*

Company Overview and Background

Trustmi is a SaaS platform that helps companies to reduce B2B fraud risk. It integrates with existing payment processes and uses AI to assist finance teams in preventing fraudulent events, managing high volumes of information, and maintaining daily operations efficiently.

In 2022, payments have become a vulnerable attack surface. Digital transformations are rapidly changing the way businesses process and manage payments. Payments are now mostly digitized, supporting a complicated supply chain, managed through a growing number of inconsistent tools and platforms that evolve quickly with the growing needs and complexity of the modern payments' ecosystem. Yet, existing controls and tools lag behind, making payments impossible to be managed by security and treasury teams.

Trustmi have identified that the root cause behind payment fraud and the accelerating trend is that organizations lack the ability to validate account details before processing payments, and that is where Trustmi comes into play to verify & validate payment transactions and vendor identities.

Trustmi secures organizations' funds from cyber-attacks, internal collusion, and human error based on a trust network with a multi-layer technology that combines the latest breakthroughs in active learning and crowdsourcing providing a comprehensive solution to payments fraud and a unique end to end solution.

Below are the most common use cases covered by Trustmi:

- Spoofed email – payment requests from unauthorized or malicious addresses
- Business email compromise – payment request from a compromised supplier
- Insider Fraud - Insider collaborating with an external supplier to falsify payments
- Human error - wrong payment amounts or payments to wrong accounts
- Financial system attack – compromised user with access to an accounting system, being used to change vendor’s account numbers or other critical details.
- Executive fraud – email impersonation to one of the organization’s executives followed by an urgent request for wire transfer, payments, other actions.

Products and Services

- Trustmi Detect – is a core engine which detects payment risk, suspicious transactions or vendors and potential fraud ensuring that all payments are routed to the correct destination and that the payment process remains intact. Trustmi platform empowers the user with complete visibility & control over the full payment matrix, connecting all the dots within the various organization silos to create a transparent and secure payment flow within the company, each transaction within the system receives a trust verdict with an indicator representing its risk score providing the user with actionable verdict allowing them to take an action and respond before the payment is approved.

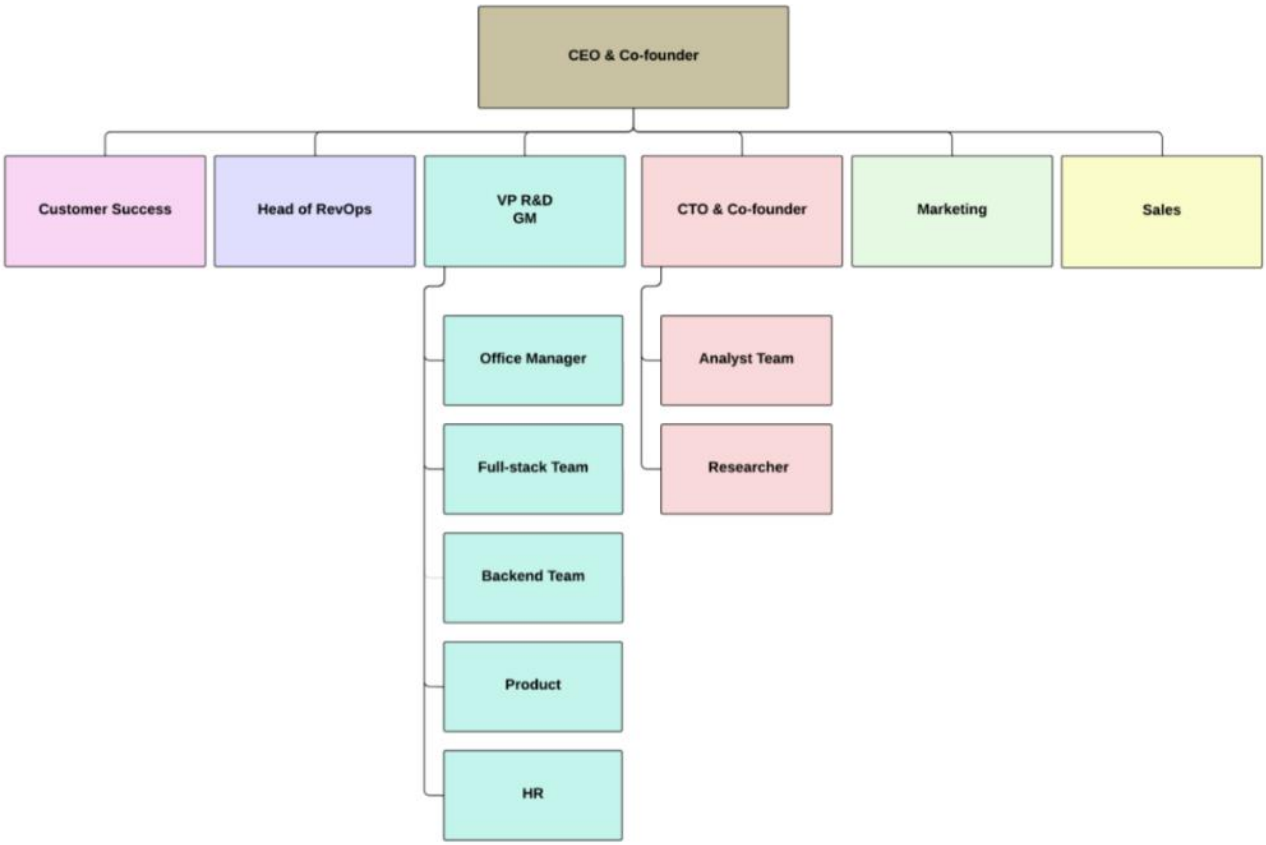
- TRUSTMI Protect - Leveraging Trustmi Detection capabilities Trustmi is able to integrate with the payments approval process and add security gates to block or prevent transactions from being approved within the payment channel. Trustmi is able to disable suspicious vendors which exhibit fraudulent activities within the trust network preventing new transactions or payments to be processed until a manual verification takes place, In addition to a simple blocking method Trustmi supports a semi-automatic flow in which an additional checks requiring a human approval as part of the traditional payment flow is managed via the platform and sent to one or both parties of the transaction to further enhance the trust level in a specific transaction or critical change request.

- TRUSTMI Certify - Trustmi provides companies with a self-service portal to enroll and verify their payment and contact details. Once those details are vetted by Trustmi, they could use the portal as a trusted certificate and use it as a verified source of truth for their customers & vendor. This certificate and public records reduce the onboarding hassle as it relates to questions and proof of identity requirements. As an added value feature once, the details need to be altered changing them in Trustmi portal will trigger a trusted notification to all customers & vendors working with the customer that a legitimate change has been processed and validated by Trustmi providing an easy scalable method to validate the correct and current vendor details.

- TRUSTMI Verify - Trustmi provide companies and individuals with a self-service portal & API integration to verify vendor payment & contact details as well as validate payment-related files such as invoices. This service has two aspects one aspect is aimed to provide proof of identity while the other aspect is aimed to validate if the payment objects and related files are legitimate detecting tampering and indicating true origin.

Organizational Structure

Trustmi's organizational structure provides the overall framework for planning, directing and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. An organization chart including personnel, job titles and clear reporting hierarchy is documented. Management authorities and reporting hierarchy are clearly defined **(14).** Below is a description of key Trustmi departments:



Sales & BD: The sales department is composed of specialized and experienced sales personnel. It is responsible for selling and optimizing sales to Trustmi customers.

Marketing: The marketing department is responsible for building the company's brand, generating sales opportunities, and other marketing activities.

Operations: The operation department includes the following entities:

- *Information Technology (IT)*: The IT department is responsible for providing Trustmi with the required IT environments.
- *Security:* Responsible for the production SaaS environments availability, security and scalability.
- Security Compliance: responsible for ongoing Information Security and Privacy compliance maintenance activities.
- Support: Is responsible for providing support to Trustmi's customers. The support team works closely with Operations, R&D, QA and Professional Services departments.

Product: The product team is responsible for defining the Trustmi product lines and available services - requirements and priorities. It includes, among others, analyzing market needs and incorporating client feedback into the products roadmaps.

HR – The department is responsible mainly for the following.

- Talent Acquisition: sourcing, recruiting, and onboarding new employees, ensuring the organization has the right individuals with the necessary skills and qualifications.
- Employee Development: oversees training and development programs, enabling employees to enhance their skills, knowledge, and career growth within the company.
- HR Policies and Compliance establishes and enforces company policies, procedures, and legal compliance to maintain a fair and respectful work environment while adhering to labor laws and regulations.

Research & Development (R&D): The R&D department is responsible for developing, testing and validating Trustmi's products and the business services implemented within the production environment. This department includes eight development groups as detailed below:

- *Dev* – responsible for the development of the core services.
- *Dev2* – responsible for the development, AI and research.
- *Dev3 - responsible for the integrations with 3rd parties.*
- *Dev4 - responsible for frontend of all products*.
- *DevOps* – responsible for DevOps services.
- *Automation and QA* – responsible for automation & QA services.
- *Sustaining Engineering* – responsible for Tier4 support.

Overview of Company's Internal Control

A company's internal control is a process – affected by the entity's boards of directors, management and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the five components of internal control for Trustmi Network.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods and organizational structure. Trustmi Network's executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures. Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees within the internal portal **(2)**. Information security policy defining the company's strategic direction regarding information security aspects is documented, followed, and reviewed on an annual basis **(19).**

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through Trustmi Network's:
(1) Management operating style,
(2) Organizational structure,
(3) Employee job descriptions, and
(4) Organizational policies and procedures

Board of Directors - Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained **(12).** The Board of Directors (BOD) of Trustmi has comprised 4 directors of which 2 are appointed by CyberStarts, and two founders of the Company who also serve executive officers of the Company. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. Members of the Board meet on at least a quarterly basis to discuss matters pertinent to the Company and to review financial information. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of the Company through

its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate.

Management Philosophy and Operating Style – Management meetings are held and documented on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained **(22).** The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage Trustmi and its business daily. Trustmi is led by a team with proven ability in cyber security and Fintech solutions to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Trustmi's objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. In addition, the Management Team convenes off-site on a half-year basis for strategic purposes.

Integrity and Ethical values – Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Trustmi's ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of the organization's values and behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within Trustmi to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Human Resources Policy and Practices – Human resource policies and practices related to hiring, orienting, training, evaluating, promoting and compensating personnel. The competence and integrity of Trustmi's personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the Trustmi's policies that define how services should be delivered, and products need to be developed. These are located on the Trustmi network and can be accessed by relevant Trustmi team members while communicating by emails on an as-needed basis. Also, internal employees sign on an NDA as part of their employment contract with the Company **(51).**

Commitment to Competence - Competence at Trustmi is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. New professional employees that join Trustmi are required to attend an On-Boarding welcome session (held every 3 months) which provides them with the necessary knowledge about the firm and general work procedures. New employees go through an onboarding process in which the company communicates its values, policies, procedures and the responsibilities and requirements from new employees. Also, new employees are granted access to the different environments upon job requirements **(52).** The onboarding process includes gradual training of the new employee, using the buddy system and leveled progress in the performed tasks and gaining required permissions based on that level.

In addition, job candidates go through reference checks and a screening process to check their suitability for the company's objectives **(58).** Also, a list of available job and their descriptions is documented and maintained for each open position, and reviewed and updated within the company website **(15).**

Additionally, Trustmi 's Team Leaders are responsible for training plans for their newcomers. A professional training for existing employees is typically done only for new tools. It is the manager's role to decide what training a particular employee requires as they relate to specific job requirements. The company conducts security and privacy awareness training program to maintain security awareness posture **(53).** Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis **(138)**.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity's objectives. Trustmi's operating and functional units are required to implement control activities that help achieve business objectives associated with:
(1) The reliability of financial reporting,
(2) The effectiveness and efficiency of operations, and
(3) Compliance with applicable laws and regulations.

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

Risk Assessment

Risk identification: Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations **(11).** The process of identifying, assessing and managing risks is a critical component of Trustmi's internal control system. The purpose of Trustmi's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis embodies identification of key business processes in which potential exposures of some consequence exist. Exposures defined by Trustmi, considers both internal and external influences that may harm the entity's ability to provide reliable services. It includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and service, business partners, customers, and others with access to the Trustmi's information systems.

Risk assessment: Risk assessment meetings where stakeholders evaluate risks and threats take place and documented **(10).** The organization defines and documents a risk assessment and management policy specifying strategic directions for risk assessment. The policy should cover directions for analyzing, identifying, evaluating and addressing internal and external risks and should consider risks in all business aspects including but not limited to IT **(9).** Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of Trustmi and include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. The assessment includes how the risk should be managed and whether to accept, avoid, reduce, or share the risk. Managers of each department are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. The Management Team considers the significance of the identified risks by determining the criticality and impact of the risks. Additionally, asset inventory of hardware, servers, workstations, laptops and mobile devices is being tracked and managed **(91).**

Risk Mitigation

Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. Trustmi selects and develops control activities that contribute to the mitigation of risks to the achievement of the company's objectives to acceptable levels. The risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Trustmi's objectives during response, mitigation, and recovery efforts.

Risk responses that address and mitigate risks are carried out. The Management Team considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities. The relevant business processes are thoroughly controlled using a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. Financial impacts of the risks are also taken in consideration during the process. Vendor risk management policy is documented, and the policy defines how the company evaluates, engages, and provisions new and existing vendors. The policy reviewed and approved by the Trustmi management on an annual basis **(5).** Trustmi assesses the risks associated to their vendors and business partners on a periodic basis. Also, prior to engaging with third-party vendors an NDA must be signed **(23)**. Vendor risk management policy is documented and the policy defines how the company evaluates, engages, and provisions new and existing vendors **(5)**. Moreover, the company evaluates risks regarding vendors, partners, subcontractors, infrastructure providers and other related third-parties, including review of the security compliance reports. Deviations are investigated. The review includes identifying and documenting the controls in place to address the CUECs **(6).**

Information and Communication

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

System description and boundaries are documented and communicated to both internal and external parties; to employees through the internal portal or a shared folder, and to customers and partners through the emails **(8).** Weekly meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives. Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate Trustmi personnel via email messages and shared with appropriate audience through the use of the internal communication tool. Availability, confidentiality and security related obligations are communicated to Trustmi's employees through the confidentiality and non-disclosure agreements while client obligations and commitments are communicated within the contracts. New features are communicated to customers, through the external portal **(119).** In addition, Trustmi's approved policies as well as the process of informing the entity about breaches of the system Security, Availability and Confidentiality are communicated to personnel responsible for implementing them in the internal application.

General Company Policies

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand Trustmi's objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. In addition, Responsibility and accountability for developing and maintaining the policies are assigned to the Trustmi relevant teams and are reviewed and approved on an annual basis by the management team.

Logical and Physical Access

Trustmi 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. Information security policy defining the company's strategic direction regarding information security aspects is documented, followed, and reviewed on an annual basis **(19).**

Access Control, User and Permissions Management

Trustmi builds its production environment system architecture using the AWS services. Firewall detailed configuration is defined and performed by the Trustmi Operations team. In addition, the global management of the Trustmi infrastructure is performed by Trustmi using a dedicated AWS workspace. This interface allows Trustmi to, among others, (1) add, modify and manage servers, (2) create security policies as they relate to these servers, (3) configure a few network and firewall parameters, (4) manage the databases and (5) manage the AWS users. Firewalls separate the internal network from the internet. Firewall settings have been configured to allow only authorized traffic, as defined in Trustmi 's Security Policy.

Trustmi manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data. Authorized access to the AWS' hosting environment is performed only through Bastion Host restricted to Trustmi's VPN to servers' farm by using SAML authentication and two factors authentication. The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel (refer to section 'Production Environment Logical Access).

Several controls are in place to ensure that access management is properly done:

- Access to system resources is protected through a combination of firewalls, VPNs, native operating system access controls, database management system security, application controls and intrusion detection monitoring software **(131).**
- Strong password policy is configured and enforced for cloud providers and sensitive SaaS tools such as source control, build tool and identity management tool, including password length, complexity, change intervals, non-defaults and login attempts limitation **(65).**
- Multi-factor authentication (MFA) is enforced and enabled for all users on cloud provider management console and sensitive SaaS applications such as source control, build tool and identity management tool **(76).**
- A network firewall is configured and operating on production environments to prevent malicious network access to networks and machines **(87).**
- Sensitive SaaS application access permissions are restricted to authorized users only, for the source control, build, and identity management tools **(34).**
- Production environment access permissions are restricted to authorized users only. Specific developers can be granted temporary access for specific projects. The accesses are logged and reviewed **(33).**
- Access to personal information in databases is restricted to authorized Company's personnel **(109).**
- Permissions for development tools, including source control and CI/CD, are restricted to authorized users only **(60).**
- Permissions for approving merge requests are restricted to authorized personnel **(67).**

Recertification of Access Permissions

User access permissions review process for cloud environments, servers, application and SaaS applications is performed every six months by the relevant resource owner **(35).** Trustmi has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments and databases. Employees

whose job functions have changed and therefore no longer require access to a group of user permissions will have their access disabled or modified as needed.

Revocation Process

Terminated employees go through an off-boarding process with a clear off-boarding checklist and have no access permission to the production environment and other applications **(57).** Terminated employees complete a termination clearance process on their last day at Trustmi while the termination notification is documented and accessible within the Trustmi Internal IT management ticket system. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data and equipment.

Production Environment Logical Access

The production environment is separated into Virtual Private Cloud (VPC) which are assigned to customers. Access to the customer environment web application interface is performed using personal production username and password for relevant users. Admin access to the AWS servers is performed using a VPN, which is uniquely identified at the AWS datacenter. This access still requires a specific production username and password, which is available to each relevant user. The access to the Production servers is performed by using SSH keys and is restricted to authorized personnel.

Employees are provided with the minimal access rights required to carry out their duties. New users accessing Trustmi system are granted access upon notification from the direct manager. A detailed ticket is opened in the IT management ticketing system using a new hire template. This template includes all user detailed permissions.

Remote Access

Trustmi's production environment servers are hosted in AWS and protected by AWS tools and controls configured by Trustmi and protected using commercial firewalls configured and administered by the IT department. Direct remote access to production servers is restricted and performed through a dedicated jump server (bastion host) or VPN **(75).** Trustmi employees are granted remote access to the production network environment based on the need-to-work principle. Traffic entering Trustmi's production network is monitored and screened by a firewall and monitoring tools implemented by AWS and configured by Trustmi. Remote users are automatically disconnected from the production servers after a pre-defined period of inactivity and need to login again in order to re-establish connection to the network.

Physical Access and Visitors

Trustmi recognizes the significance of physical security controls as a key component in its overall security program. Physical access to offices is restricted to authorized personnel only. Also, visitors to the Trustmi office are accompanied while on premises **(81).** Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas. These access chips and keypad codes are issued to Trustmi 's employees by the administrative manager. Permissions to issue them and grant access are restricted to the administrative manager and the authorized designees.

Software Development Lifecycle (SDLC) Overview

The software development lifecycle consists of the following stages:

- Product/Engineering Requirements Definition
- Detailed Design
- Coding
- Unit Testing
- Integration Testing
- System Testing
- SAST scanning
- Beta Release

- General Availability (GA) Release

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. Product requirements are constantly being collected from customers and from market research by Trustmi Product Managers. These requirements combined with additional engineering improvement requirements are discussed by R&D managers and Product Managers and are converted to a Product Requirements Document (PRD) that contains more specific description of required features and changes.
The R&D Managers review the PRD and provide a high-level effort estimation for every feature. The product managers work with the R&D managers to create a prioritized features list based on the effort estimation and required timeline of the release. The Release Manager collects the features list, validates the total effort vs teams foreseen progress and creates a release plan specifying integration dates, Feature Freeze and Code Freeze dates as well as the release date of 1st release candidate to PS. Changes in software are documented and prioritized using a change management tool and assigned to the relevant stakeholder. Each code change in the source control tool should be linked to the ticket documenting that change and vice versa. Changes are documented and prioritized using agreed communication channels **(59).** Code changes are reviewed along with the pull request and approved by professional authorized user before being merged to production. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment **(61).**

R&D Engineers are engaged with ongoing enhancements of the product functionality. Each engineer implements Unit Testing to every new coded software module in accordance with Unit Tests guidelines document. Trustmi performs unit testing using a dedicated tool. R&D engineer's check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes which are added to the Source Control contain information linking them to the relevant features and bugs. Unit Tests are maintained according to product changes and enhanced based on bugs that were detected in previous product versions. Check-in of code triggers Unit testing process and if passed successfully, a new build is created, and automated tests are executed on it.

Software quality Process: Trustmi Quality Assurance (QA) is constantly involved from early development stages. Based on the PRD, QA creates internal test plans. Testing procedures including unit testing and end-to-end testing are in place, automatically or manually **(69).** Test plans are reviewed by Product Managers and by R&D Team Leader responsible for the feature design. Each build goes through an automated pass/fail sanity testing process during which it is determined if it is acceptable to commence a full QA cycle. A full QA cycle (Stabilization) includes regression and progression tests according to test plan documents. During this stage bugs are reported in the change management tool. Each bug is assigned to an R&D Engineer for resolving with severity and a target version. Bugs that were targeted to the current version are fixed and verified as closed or are reopened. During Code Freeze, only Show Stopper bugs are fixed by the engineers.

Software Release: The official release of a version from Trustmi development should qualify by the Release Exit Criteria. It is mandatory that all automation tests pass and that scans are free of Critical and High findings. Trustmi secured development process also includes a yearly pen testing of which findings are fixed in the following release. The released version is verified by the team leader and Analyst prior to releasing to Beta customers. Show stopper bugs are reported and fixed in a new Release Candidate. A Beta version is released to selected customers. Customers who receive Beta version are notified in advance and express their wish to actively participate in this stage. The Beta version is used in standard operational environments of these customers. Bugs or functional requests that are made by customers are reported in Jira and marked with customer tag. Faults reported during this stage are analyzed by R&D and if defined as showstoppers, they will be fixed for the General Availability (GA) release. Requests for functional enhancements are going to Product Managers backlog for future Releases. A General Availability (GA) version is released as a complete installation package including Built-in help, Administration Guide and Release Notes documents. A "release exit" checklist is filled by Trustmi before releasing a version to production.

Monitoring the Change Management Processes

A change management meeting is performed before every release and as part of sprint planning, to assess the risks identified and review changes required to the production environment. Action items are updated within as part of the process and change is approved only after review and assessment. In addition, metric reports are regularly issued to the Management Team in order to provide them with key indicators regarding the change management process.

Infrastructure Change Management Overview

Trustmi regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration policies of the existing servers or performing routine maintenance activities, software updates, and other infrastructure-related changes accordingly to available possibilities provides by the third-party vendors. Infrastructure changes are documented within the Change Management process. The request is reviewed and approved by the Lead DevOps. Infrastructure changes are documented, prioritized and tracked. Changes are approved by authorized personnel **(137)**.

Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

Description of the Production Environment

The processes described below are executed within Trustmi 's production environment, hosted in co-location data centers by a third-party vendor. Amazon Web Services in the United States (N. Virginia).

AWS: Trustmi 's infrastructure runs on top of AWS's Infrastructure as a Service (IaaS) and utilizes various services such as: (1) EC2, (2) S3, (3) RDS (4), Amazon DocumentDB, (5) EKS, and more. These services are designed to make web-scale computing easier for Trustmi.
AWS's web service interface (AWS Console) allows Trustmi to obtain and configure capacity. It provides Trustmi with control of computing resources and runs on AWS's computing environment. EC2 reduces the time required to obtain and boot new server instances to minutes, allowing to quickly scale capacity, both up and down, as computing requirements change. The use of EC2 allows to:

- Select a pre-configured template to get up and running immediately or create a per-need AMI containing Trustmi - configured applications, libraries, data, and associated configuration settings.
- Configure security and network access on the EC2 instance.
- Choose which instance type(s), then start, terminate, and monitor as many instances as needed, using the web service APIs.
- Determine whether to run in multiple locations, utilize static IP endpoints, or attach persistent block storage to instances.

Production Environment

The processes described below are executed within Trustmi's production environment, which is hosted in Amazon Web Services (AWS) Virtual Private Cloud located globally. The facilities comply with standards of quality, security, and reliability that enable Trustmi to provide its' services in an efficient and stable manner.
Note: Controls performed by the data center service providers are not included in the scope of this report. The production environment is completely separated from the corporate environment and follows strict access and data processing procedures and processes. The environment is managed by a selected few Security personnel who use 2FA to connect using a dedicated AWS workspace.
All Trustmi users who connect to the customers' VPCs for support purposes should login via a named workspace. All authentication is performed with a SAML provider. Customers' data is encrypted at rest and in transfer. Access of Trustmi personnel as well as customers is further restricted by IP filtering.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the Trustmi cloud service components. To provide sufficient capacity, the Trustmi network infrastructure relies on platforms provided by Amazon Web Services (AWS). To ensure appropriate network security levels, Trustmi security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality, integrity and availability. Trustmi'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)

Web, Application and Service Supporting Infrastructure Environment

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

Production Monitoring

Trustmi uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules. Trustmi's production network encompasses numerous components including web services, application and data server types, database, monitoring tools, and redundant network equipment provided as part of the AWS services. In addition, in order to improve service availability to clients and to support the operations of the Trustmi environments, Trustmi maintains a set of automated monitoring tools and alerts on various security issues.

Monitoring Usage

Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients **(113).** The management team is updated on an annual basis on security, confidentiality and availability non-compliance issues that may come up and address them as needed. Such issues are documented as part of a support process and if necessary, notifications are sent to the Security team or the IT and Information Security Director. Change reports, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability and confidentiality policies. In addition, environmental, regulatory and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members. User log activity auditing and audit trail for database, servers, and applications is performed and reviewed at least annually **(111).**

Security and Architecture

Trustmi provides a secure, reliable and resilient Software-as-a-Service platform that has been designed from the ground up based on industry best practices. The below addresses the network and hardware infrastructure, software and

information security elements that Trustmi delivers as part of this platform, database management system security, application controls and intrusion detection monitoring software.

Data Center Security

Trustmi relies on Amazon Web Services global infrastructure, including 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: FedRAMP, HIPAA, ISO 27001:2015, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS and more. 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 has been installed to reduce risk.
- **Redundant Power** - the data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up 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.

Infrastructure Security

- **End-to-End Network Isolation** - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud being intercepted.
- **External & Internal enforcement points** - All servers are protected by restricted AWS firewall rules. The configuration of AWS firewall rules is restricted to authorized personnel.
- **Server Hardening** - all servers are hardened according to industry best practices.
- **Segregation Between Office and Production Networks** - Separate environments are used for production and development (including testing and staging). To ensure segregation of duties, entities with access to the development environments have no access to production environment **(106).** There is a complete separation between the Trustmi Corporate network and the Production network. Access to the production environment is granted to authorized personnel only, and traffic between the networks is sent over an encrypted tunnel.

Application Security

- **Penetration Testing** - Penetration tests are performed annually on products on an annual basis and high and critical issues are documented, tracked, investigated and resolved **(116).** The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on a semi-annual basis. The penetration tests and security scans are performed by a reputable third-party vendor.
- **Vulnerabilities Management** - Automated source code vulnerability scans are performed for each merge to default branches in an attempt to identify and fix security-related weaknesses (flaws) in the code **(77).** Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection).
- **Segregation of Customer Data** - Trustmi employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated by third-party security consultants on a yearly basis.

Operational Security

- **Configuration and Patch Management** - Trustmi architecture design enforce lunching up to date patched servers using AWS AMIs. Monthly maintenance includes systems review including dedicated servers OS patches (ex. Bastion host).
- **Security Incident Response Management -** Incident response is documented to contain, remediate and communicate security incidents. Incident response processes are in place to continuously evaluate, escalate and remediate security issues. Whenever a security incident of a physical or electronic nature is suspected or confirmed, Trustmi 's engineers are instructed to follow appropriate procedures. Customers and legal authorities will be notified as recurred by Privacy regulations.

- **Anti-malware** - Anti-malware software is installed on workstations, laptops, and servers supporting such software. The anti-malware software is configured to periodically receive updated virus signatures **(78).** Anti-malware software is installed on workstations, laptops, and servers supporting such software definition updates are performed and monitored on a regular basis by the IT and Operations teams. The employees' laptops are encrypted with the use of a 256-bit AES encryption.
- **Unified Endpoint Management** - Trustmi use a dedicate tool that implemented an Agent in advance on the company's endpoint in order to monitor and control the updates, data, content, configuration and encryption of the asset. The company Security Policy is enforced using a dedicate tool.

Human Resource Security

- **Security Awareness Training** - Trustmi's employees undergo an information security awareness training upon joining the company, as well as periodically in conformance to Trustmi's information security policy. The training ensures that each group of employees receive security training according to its technical knowledge and its needs.
- **Secure Coding Standards and Training** - Trustmi's R&D team is regularly trained in secure coding practices. Furthermore, it is involved with analyzing penetration test results and defining the 'lessons learned'.

Support

Trustmi's customer support procedures executed by the customer success and support teams are focused on providing the best possible experience and outcome of using the Trustmi platform and engaging with the company. Customer support mechanism is available to customers through a dedicated communication channel **(16).** Customer support mechanism is available to customers through a dedicated communication channel. The support level is directly tied to the license tier. Customers can engage with the technical experts at Trustmi through email, Slack or remote sessions. System uptime is defined in the SLA document and is being tracked and monitored **(120).**

Ticketing and Management

Trustmi opens a ticket when an issue is raised by a client or when an issue is proactively identified. Trustmi uses a third-party support application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution.

Incident Management Process

A help-desk application is available to Trustmi employees in order to report breaches in system security, availability, and confidentiality. New employees are trained in the use of this application at the beginning of their employment. The process is initiated when a new ticket is submitted in the helpdesk application or through emails. The company has a procedure and process in place to raise and manage Information Security Incidents. Incidents are classified according to the level of urgency and importance. Incidents can be submitted into the system following a customer-identified issue, through both manual and automated proactive checks, or automatically through an email request. The application has pre-defined steps that are assigned to a pre-defined group of employees. The completion of each step is recorded in the

application. When an incident is submitted, an email is sent to the IT and Information Security Director. Resources are allocated in order to investigate the incident and resolve the issue. The IT and Information Security Director is responsible for escalating critical incidents and perform Lesson Learnt reviews. By procedure and according to a strict SLA, Incident notifications are sent to customers in the case that their data has been impacted.

Escalation Process

Trustmi's goal is to resolve issues in an efficient manner. The issue is tracked and updated in the support ticketing system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to Security, R&D or Technical Services teams. Service interruptions are communicated to clients using a status page (with an e-mail subscription option). Service interruptions, maintenance and updates are communicated to customers through emails, status page link, chat or other means of communication **(13).** Support tickets escalation procedures and Service Level Agreement (SLA) notification thresholds. In addition, to maintain visibility on current support issues and potential problem trends, support metrics (including Key Performance Indicators) are generated from the support application and sent to Company's stakeholders on a regular basis.

Availability Procedures

Trustmi's production environment is fully managed as part of the AWS services and monitored by Trustmi Operation team using the tools provided by AWS as well as internal tools. The application level is fully managed by the Trustmi Security team. Trustmi has implemented the operations management controls described below to manage and execute production operations.

Database Backup

Trustmi's databases are hosted at AWS and fully on a weekly and monthly basis. The backup system automatically generates a backup log. In case of failure, a notification is sent to the Operation team. The company hold replica to each data center for high-availability standards in case of a disaster. Production databases are automatically backed up in high granularity **(27)**.

Restoration

Backup data captured as part of the daily, weekly and monthly backup procedures is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A log of the restoring process is sent to the Director of Operations for review. Database backup restoration tests are performed to validate the effectiveness of the automated database backup process **(26)**.

Data center availability procedures

AWS provides Trustmi with a secured location implementing security measures to protect against environmental risks or disaster. Production databases are located in more than one availability zone to ensure high availability **(25)**.

Business Continuity Plan (BCP)

Trustmi has developed a Business Continuity Plan to enable the company to continue to provide critical services in case of a disaster. Trustmi maintains a backup server's infrastructure at a separate location within the AWS environments. The backup server's infrastructure has been designed to provide clients with business-critical services until the disaster has been resolved and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate Trustmi personnel, as is the case with the primary production environment. Backup and disaster recovery plan policy is documented, reviewed, and tested periodically. The policy defines the company's data backup and disaster recovery directions to assure the company keeps providing required services in case of a disaster **(28)**.

Monitoring Usage

The management team is updated on an annual basis on security, confidentiality and availability non-compliance issues that may come up and address them as needed. Such issues are documented as part of a support process and if necessary notifications are sent to the Security team or the IT and Information Security Director. Change reports, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability and confidentiality policies. In addition, environmental, regulatory and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members.

Confidentiality Procedures

Customer confidentiality is key factor in Trustmi. As such, Trustmi has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. In addition, connections to the Trustmi network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Following the confidentiality measures :

- Databases residing in production environments, including backups, are encrypted at rest **(32)**.
- Customer and user passwords are encrypted or hashed, either in storage or by using a third-party user management tool that complies with this requirement **(93)**.
- Data in transit between application and customer is encrypted using TLS (minimum version 1.2) **(94)**.
- Device storage, including for laptops and workstations, is encrypted by automatic software to restrict access to sensitive information **(74)**.
- Server disks residing in production environments, including backups, are encrypted at rest **(43)**.
- Access keys, secret keys, API keys and other cryptographic keys are stored securely, rotated, and protected **(96)**.
- Buckets residing in production environments, including backups, are encrypted at rest **(54)**.

Privacy Procedures

Management

Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating Trustmi's privacy policies. The names of such persons or groups and their responsibilities are defined **(97).** Trustmi implements security awareness training to help ensure that company employees are aligned with security practices and are aware of their duties with regard to data privacy. The training details the secure handling of company confidential information, including customer data. The mandatory training is conducted for new and existing employees.

Information Lifecycle

The collection and processing of personal information is consistent with the company's privacy commitments and system requirements **(100).** Customer contracts include privacy considerations on which the customer signs and acknowledge how its personal data is collected and used **(95).** The company securely retains personal information to meet the entity's objectives related to privacy **(132).** In addition, the company securely disposes of personal information to meet the entity's objectives related to privacy **(99).**

Notice

An up-to-date privacy policy is available on the company's website, and reviewed and updated by management. The policy outlines how the company handles private data and fully discloses the types of information the company may collect via its products and website, as well as how it may use this information **(101).** Privacy statement informing customers the types of collected data and how this data is used is provided in the company's website and application and reviewed periodically **(107).**

Privacy by Design

To help ensure the delivery of security services to customers, security and privacy by design are an inherent part of Trustmi's Secure Software Development Life Cycle. For applications to be designed and implemented with proper security requirements, secure coding practices that focus on privacy and security risks are integrated into day-to-day operations and in the development processes. Changes affecting the level of security, privacy, availability, and confidentiality issues within the production environment are reviewed as part of risk assessment sessions.

Data Subject Rights and Dispute Resolution

The company implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entits objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner **(135).** The company grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entitys objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entitys objectives related to privacy **(103).** In addition, The company corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entitys objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entitys objectives related to privacy **(133).**

Disclosure to Third Parties

The company creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entitys objectives related to privacy **(136).** Third parties requiring access to company's private data provide privacy obligations through privacy standards or signed contracts. The entity assesses those parties compliance on a periodic and as-needed basis and takes corrective action, if necessary **(104).**

Breach Management

The company provides notification of data (including personal data) breaches and incidents, to the affected data subjects, regulators, and others **(134).** The company grants identified and authenticated data subjects the ability to opt-out and to erase their stored data in the company's applications **(105).**

Subservice Organization carved-out controls: Amazon Web Services ('AWS')

The subservice organization is 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 the access to the virtual and physical servers, software, firewalls and physical storage to authorized individuals and to 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 as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, related policies.
- Provide that only authorized tested and documented changes are made to the system.

Trustmi' customers' responsibilities

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Trustmi.
- 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 Trustmi' services.
- Maintaining authorized, secure, timely, and complete transactions for user organizations relating to Trustmi services.
- Protecting data that is sent to Trustmi by using appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- Implementing controls requiring additional approval procedures for critical transactions relating to Trustmi services.
- Reporting to Trustmi in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Trustmi.
- Notifying Trustmi in a timely manner of any changes to personnel directly involved with services performed by Trustmi. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Trustmi.
- Adhering to the terms and conditions stated within their contracts with Trustmi.
- Developing, and if necessary, implementing a business continuity and disaster recovery plan (DRP) that will aid in the continuation of services provided by Trustmi.

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

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing, and extent of its testing of the controls specified by Trustmi, Kost Forer Gabbay and Kasierer (KFGK) considered the aspects of Trustmi's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system- generated populations for sample-based testing), we 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) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and 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 Trustmi Network Ltd. The testing performed by KFGK and the results of tests are the responsibility of the service auditor.

Control Environment

CC1.1 / COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
19	Information security policy defining the company's strategic direction regarding information security aspects is documented, followed, and reviewed on an annual basis.	Inspected the Information security policy and determined that an Information security policy defining the company's strategic direction regarding information security aspects was documented, followed, and reviewed on an annual basis.	No deviations noted.

CC1.2 / COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that the board met at least on a quarterly basis, documented and had a fixed agenda. Meeting minutes were retained.	No deviations noted.

CC1.3 / COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
12	Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that the board met at least on a quarterly basis, documented and had a fixed agenda. Meeting minutes were retained.	No deviations noted.
14	An organization chart including personnel, job titles and clear reporting hierarchy is documented. Management authorities and reporting hierarchy are clearly defined.	Inspected Trustmi's organizational chart and determined that an organizational chart including personnel, job titles and clear reporting hierarchy was documented. Management authorities and reporting hierarchy were clearly defined.	No deviations noted.
22	Management meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected the management meeting minutes and invitations and determined that the management of the company met on a quarterly basis to discuss ongoing issues and updates. Meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity’s privacy policies.	No deviations noted.

CC1.4 / COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	A list of available job and their descriptions is documented and maintained for each open position and reviewed and updated within the company website.	Inspected a sample of job descriptions and determined that the job descriptions were reviewed and updated annually, documented and maintained within the company website.	No deviations noted.
58	Job candidates go through reference checks and a screening process to check their suitability for the company's objectives.	For a sample of new employees, inspected the reference checks documentation and determined that job candidates went through reference checks and a screening process to check their suitability for the company's objectives.	No deviations noted.
52	New employees go through an onboarding process in which the company communicates its values, policies, procedures and the responsibilities and requirements of new employees. Also, new employees are granted access to the different environments upon job requirements.	For a sample of new employees, inspected the onboarding tickets and determined that new employees went through a dedicated onboarding process in which the company communicated its values, policies, procedures and the responsibilities and requirements of new employees. Also, New employees were granted access to the different environments upon job requirements.	No deviations noted.
53	The company conducts security & privacy awareness training program to maintain security awareness posture.	For a sample of current employees, inspected the examination certificates and the training materials and determined that the company conducted security & privacy awareness training program to maintain security awareness posture.	No deviations noted.

CC1.5 / COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
14	An organization chart including personnel, job titles and clear reporting hierarchy is documented. Management authorities and reporting hierarchy are clearly defined.	Inspected Trustmi's organizational chart and determined that an organizational chart including personnel, job titles and clear reporting hierarchy was documented. Management authorities and reporting hierarchy were clearly defined.	No deviations noted.
53	The company conducts security & privacy awareness training program to maintain security awareness posture.	For a sample of current employees, inspected the examination certificates and the training materials and determined that the company conducted security & privacy awareness training program to maintain security awareness posture.	No deviations noted.

Communication and Information

CC2.1 / COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	The organization defines and documents a risk assessment and management policy specifying strategic directions for risk assessment. The policy should cover directions for analyzing, identifying, evaluating and addressing internal and external risks and should consider risks in all business aspects including but not limited to IT.	Inspected the risk assessment and management policy and determined that the organization defined and documented a risk assessment and management policy specifying strategic directions for risk assessment. The policy should have covered directions for analyzing, identifying, evaluating and addressing internal and external risks and should have considered risks in all business aspects including but not limited to IT.	No deviations noted.
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	No deviations noted.

CC2.2 / COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
52	New employees go through an onboarding process in which the company communicates its values, policies, procedures and the responsibilities and requirements of new employees. Also, new employees are granted access to the different environments upon job requirements.	For a sample of new employees, inspected the onboarding tickets and determined that new employees went through a dedicated onboarding process in which the company communicated its values, policies, procedures and the responsibilities and requirements of new employees. Also, new employees were granted access to the different environments upon job requirements.	No deviations noted.
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity’s privacy policies.	No deviations noted.
53	The company conducts security & privacy awareness training program to maintain security awareness posture.	For a sample of current employees, inspected the examination certificates and the training materials and determined that the company conducted security & privacy awareness training program to maintain security awareness posture.	No deviations noted.
8	System description and boundaries are documented and communicated to both internal and external parties; to employees through the internal portal, and to customers and partners through emails.	Inspected the network diagram, the architecture overview and determined that system description and boundaries were documented and communicated to internal parties through the internal portal.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected a sample of emails and determined that system description and boundaries were documented and communicated to external parties through emails.	

CC2.3 / COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	Service interruptions, maintenance and updates are communicated to customers through emails, status page links, chat or other means of communication.	Inspected the company's status page and determined that service interruptions, maintenance and updates were communicated to customers through a status page link. No service interruption occurred during the audit period.	No deviations noted.
120	System uptime is defined in the SLA document and is being tracked and monitored.	Inspected a sample of singed SLAs from the audit period and determined that system uptime was defined in the SLA document and was being tracked and monitored. No service interruption occurred during the audit period.	No deviations noted.
16	Customer support mechanism is available to customers through a dedicated communication channel.	Inspected Trustmi's CRM tool dashboard and a sample of customer support tickets and determined that customer support mechanism was available to customers through a dedicated communication channel.	No deviations noted.
119	New features are communicated to customers, through the external portal.	Inspected a sample of release notes and determined that new features were communicated to customers through the external portal.	No deviations noted.
8	System description and boundaries are documented and communicated to both internal and external parties; to employees through the internal portal, and to customers and partners through emails.	Inspected the network diagram, the architecture overview and determined that system description and boundaries were documented and communicated to internal parties through the internal portal. Inspected a sample of emails and determined that system description and boundaries were documented and communicated to external parties through emails.	No deviations noted.

Risk Assessment

CC3.1 / COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	Vendor risk management policy is documented, and the policy defines how the company evaluates, engages, and provisions new and existing vendors.	Inspected the company's vendor risk management policy and determined that a vendor risk management policy was documented and the policy defines how the company evaluated, engaged, and provisioned new and existing vendors.	No deviations noted.
9	The organization defines and documents a risk assessment and management policy specifying strategic directions for risk assessment. The policy should cover directions for analyzing, identifying, evaluating and addressing internal and external risks and should consider risks in all business aspects including but not limited to IT.	Inspected the risk assessment and management policy and determined that the organization defined and documented a risk assessment and management policy specifying strategic directions for risk assessment. The policy should have covered directions for analyzing, identifying, evaluating and addressing internal and external risks and should have considered risks in all business aspects including but not limited to IT.	No deviations noted.
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	No deviations noted.

CC3.2 / COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that the board met at least on a	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		quarterly basis, documented and had a fixed agenda. Meeting minutes were retained.	
22	Management meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected the management meeting minutes and invitations and determined that the management of the company met on a quarterly basis to discuss ongoing issues and updates. Meeting minutes were retained.	No deviations noted.
5	Vendor risk management policy is documented, and the policy defines how the company evaluates, engages, and provisions new and existing vendors.	Inspected the company's vendor risk management policy and determined that a vendor risk management policy was documented and the policy defines how the company evaluated, engaged, and provisioned new and existing vendors.	No deviations noted.
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity’s privacy policies.	No deviations noted.
9	The organization defines and documents a risk assessment and management policy specifying strategic directions for risk assessment. The policy should cover directions for analyzing, identifying, evaluating and addressing internal and external risks and should consider risks in all business aspects including but not limited to IT.	Inspected the risk assessment and management policy and determined that the organization defined and documented a risk assessment and management policy specifying strategic directions for risk assessment. The policy should have covered directions for analyzing, identifying, evaluating and addressing internal and external risks and should have considered risks in all business aspects including but not limited to IT.	No deviations noted.
10	Risk assessment meetings where stakeholders evaluate risks and threats take place and documented.	Inspected the risk assessment meeting invitations and minutes and determined that a risk assessment meeting took place on an annual basis and was documented.	No deviations noted.
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	

CC3.3 / COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that the board met at least on a quarterly basis, documented and had a fixed agenda. Meeting minutes were retained.	No deviations noted.
22	Management meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected the management meeting minutes and invitations and determined that the management of the company met on a quarterly basis to discuss ongoing issues and updates. Meeting minutes were retained.	No deviations noted.
9	The organization defines and documents a risk assessment and management policy specifying strategic directions for risk assessment. The policy should cover directions for analyzing, identifying, evaluating and addressing internal and external risks and should consider risks in all business aspects including but not limited to IT.	Inspected the risk assessment and management policy and determined that the organization defined and documented a risk assessment and management policy specifying strategic directions for risk assessment. The policy should have covered directions for analyzing, identifying, evaluating and addressing internal and external risks and should have considered risks in all business aspects including but not limited to IT.	No deviations noted.
10	Risk assessment meetings where stakeholders evaluate risks and threats take place and documented.	Inspected the risk assessment meeting invitations and minutes and determined that a risk assessment meeting took place on an annual basis and was documented.	No deviations noted.
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	

CC3.4 / COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
26	Database backup restoration tests are performed to validate the effectiveness of the automated database backup process.	Inspected the restore test documentation and determined that the database backup restoration tests were performed to validate the effectiveness of the automated database backup process.	No deviations noted.
6	The company evaluates risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations are investigated. The review includes identifying and documenting the controls in place to address the CUECs.	Inspected the vendor risk assessment matrix documentation and determined that the company valuated risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations were investigated. Inspected the infrastructure provider SOC 2 report review and determined that it included identifying and documenting the controls in place at to address the CUECs.	No deviations noted.
9	The organization defines and documents a risk assessment and management policy specifying strategic directions for risk assessment. The policy should cover directions for analyzing, identifying, evaluating and addressing internal and external risks and should consider risks in all business aspects including but not limited to IT.	Inspected the risk assessment and management policy and determined that the organization defined and documented a risk assessment and management policy specifying strategic directions for risk assessment. The policy should have covered directions for analyzing, identifying, evaluating and addressing internal and external risks and should have considered risks in all business aspects including but not limited to IT.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	No deviations noted.

Monitoring Activities

CC4.1 / COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
111	User log activity auditing and audit trail for database, servers, and applications is performed and reviewed at least annually.	Inspected a sample of access logs to production, DB, backup, and application and determined that user log activity auditing and audit trail for database, servers, and applications was performed. Inspected a sample of audit alerts and determined that the logs were reviewed at least annually.	No deviations noted.
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients.	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		notified of events related to the security, availability, or confidentiality of service to clients.	
120	System uptime is defined in the SLA document and is being tracked and monitored.	Inspected a sample of singed SLAs from the audit period and determined that system uptime was defined in the SLA document and was being tracked and monitored. No service interruption occurred during the audit period.	No deviations noted.

CC4.2 / COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	Service interruptions, maintenance and updates are communicated to customers through emails, status page links, chat or other means of communication.	Inspected the company's status page and determined that service interruptions, maintenance and updates were communicated to customers through a status page link. No service interruption occurred during the audit period.	No deviations noted.
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients.	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were notified of events related to the security, availability, or confidentiality of service to clients.	No deviations noted.
10	Risk assessment meetings where stakeholders evaluate risks and threats take place and documented.	Inspected the risk assessment meeting invitations and minutes and determined that a risk assessment meeting took place on an annual basis and was documented.	No deviations noted.

Control Activities

CC5.1 / COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	No deviations noted.

CC5.2 / COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies.	No deviations noted.
53	The company conducts security & privacy awareness training program to maintain security awareness posture.	For a sample of current employees, inspected the examination certificates and the training materials and determined that the company conducted security & privacy awareness training program to maintain security awareness posture.	No deviations noted.

CC5.3 / COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis. Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	No deviations noted.
14	An organization chart including personnel, job titles and clear reporting hierarchy is documented. Management authorities and reporting hierarchy are clearly defined.	Inspected Trustmi's organizational chart and determined that an organizational chart including personnel, job titles and clear reporting hierarchy was documented. Management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Vendor risk management policy is documented, and the policy defines how the company evaluates, engages, and provisions new and existing vendors.	Inspected the company's vendor risk management policy and determined that a vendor risk management policy was documented and the policy defines how the company evaluated, engaged, and provisioned new and existing vendors.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies.	No deviations noted.

Logical and Physical Access Controls

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
33	Production environment access permissions are restricted to authorized users only. Specific developers can be granted temporary access for specific projects. The access is logged and reviewed.	Inspected the list of users with access to the production and database environments and determined that specific developers can be granted access to specific projects. Inspected a sample of access requests to the production and database environments and determined that specific developers can be granted temporary access for specific projects. Inspected the log review documentation and determined that access and changes within the production are logged and reviewed	No deviations noted.
34	Sensitive SaaS application access permissions are restricted to authorized users only, for the source control, build, and identity management tools.	Inspected the list of users with access to the sensitive SaaS application and determined that sensitive SaaS application access permissions were restricted to authorized users only, for source control, build, and identity management tools.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
60	Permissions for development tools, including source control and CI/CD, are restricted to authorized users only.	Inspected the list of users with access to development tools, including source control and CI\CD tools and determined that permissions were restricted to authorized users only.	No deviations noted.
65	Strong password policy is configured and enforced for cloud providers and sensitive SaaS tools such as source control, build tool and identity management tool, including password length, complexity, change intervals, non-defaults and login attempts limitation.	Inspected the AWS and the SSO tool password configurations settings and determined that strong password policy was configured and enforced for cloud providers and sensitive SaaS tools such as source control, build tool and identity management tool, including password length, complexity, change intervals, non-defaults and login attempts limitation.	No deviations noted.
67	Permissions for approving merge requests are restricted to authorized personnel.	Inspected the list of users with permission to approve merge requests and determined that it was restricted to authorized personnel.	No deviations noted.
75	Direct remote access to production servers is restricted and performed through a dedicated jump server (bastion host) or VPN.	Inspected the production access configurations from AWS and determined that remote access to production servers was restricted and performed through a dedicated jump server (bastion host) or VPN.	No deviations noted.
76	Multi-factor authentication (MFA) is enforced and enabled for all users on cloud provider management console and sensitive SaaS applications such as source control, build tool and identity management tool.	Inspected the MFA configuration from the SSO tool and determined that multi-factor authentication was enforced and enabled for all users on cloud provider management console and sensitive SaaS applications such as source control, build tool and identity management tool.	No deviations noted.
96	Access keys, secret keys, API keys and other cryptographic keys are stored securely, rotated, and protected.	Inspected the AWS encryption keys configurations and determined that access keys, secret keys, API keys and other cryptographic keys were stored securely, rotated, and protected.	No deviations noted.
106	Separate environments are used for production and development (including testing and staging). To ensure segregation of duties, entities with access to	Inspected the list of users with access to the production environment and determined that separate environments were used for production and development (including testing and staging). To ensure	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	the development environments have no access to production environment.	segregation of duties, entities with access to the development environments had no access to production environment.	
32	Databases residing in production environments, including backups, are encrypted at rest.	Inspected the encryption configuration and determined that databases residing in production environments, including backups, were encrypted at rest.	No deviations noted.
87	A network firewall is configured and operating on production environments to prevent malicious network access to networks and machines.	Inspected the firewall configuration and determined that network firewall was configured and operated on production environments to prevent malicious network access to networks and machines.	No deviations noted.
111	User log activity auditing and audit trail for database, servers, and applications is performed and reviewed at least annually.	Inspected a sample of access logs to production, DB, backup, and application and determined that user log activity auditing and audit trail for database, servers, and applications was performed. Inspected a sample of audit alerts and determined that the logs were reviewed at least annually.	No deviations noted.
93	Customer and user passwords are encrypted or hashed, either in storage or by using a third-party user management tool that complies with this requirement.	Inspected customer and user passwords configuration and determined that customer and user passwords were encrypted or hashed in database.	No deviations noted.
94	Data in transit between application and customer is encrypted using TLS (minimum version 1.2).	Inspected the TLS certificates and determined that data in transit between application and customer was encrypted using TLS (minimum version 1.2).	No deviations noted.
91	Asset inventory of hardware, servers, workstations, laptops and mobile devices is being tracked and managed.	Inspected the device inventory information of the company and determined that asset inventory of hardware, servers, workstations, laptops and mobile devices was tracked and managed.	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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
52	New employees go through an onboarding process in which the company communicates its values, policies, procedures and the responsibilities and requirements of new employees. Also, new employees are granted access to the different environments upon job requirements.	For a sample of new employees, inspected the onboarding tickets and determined that new employees went through a dedicated onboarding process in which the company communicated its values, policies, procedures and the responsibilities and requirements of new employees. Also, New employees were granted access to the different environments upon job requirements.	No deviations noted.
57	Terminated employees go through an off-boarding process with a clear off-boarding checklist and have no access permission to the production environment and other applications.	For a sample of terminated employees, inspected the offboarding checklist documentation and determined that terminated employees went through an off-boarding process with a clear off-boarding checklist and had no access permission to the production environment and other applications.	No deviations noted.
106	Separate environments are used for production and development (including testing and staging). To ensure segregation of duties, entities with access to the development environments have no access to production environment.	Inspected the list of users with access to the production environment and determined that separate environments were used for production and development (including testing and staging). To ensure segregation of duties, entities with access to the development environments had no access to production environment.	No deviations noted.

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	
35	User access permissions review process for cloud environments, servers, application and SaaS applications is performed every six months by the relevant resource owner.	Inspected the user access review documentation and determined that permissions within the different environments were reviewed for cloud environments, servers, application and SaaS applications by the relevant resource owner.	No deviations noted.
57	Terminated employees go through an off-boarding process with a clear off-boarding checklist and have no access permission to the production environment and other applications.	For a sample of terminated employees, inspected the offboarding checklist documentation and determined that terminated employees went through an off-boarding process with a clear off-boarding checklist and had no access permission to the production environment and other applications.	No deviations noted.
111	User log activity auditing and audit trail for database, servers, and applications is performed and reviewed at least annually.	Inspected a sample of access logs to production, DB, backup, and application and determined that user log activity auditing and audit trail for database, servers, and applications was performed. Inspected a sample of audit alerts and determined that the logs were reviewed at least annually.	No deviations noted.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	Policies and procedures are documented, reviewed, approved by the Trustmi management on an annual basis and available to employees.	Inspected the company's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the Trustmi management on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the company's internal portal and determined that policies and procedures were available to Trustmi employees within the internal portal.	
81	Physical access to offices is restricted to authorized personnel only. Also, visitors to the Trustmi office are accompanied while on premises.	Inspected the physical access policy and documentation of the entrance and determined that access was restricted to authorized personnel only. Also, visitors to the Trustmi office were accompanied while on premises.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
81	Physical access to offices is restricted to authorized personnel only. Also, visitors to the Trustmi office are accompanied while on premises.	Inspected the physical access policy and documentation of the entrance and determined that access was restricted to authorized personnel only. Also, visitors to the Trustmi office were accompanied while on premises.	No deviations noted.
6	The company evaluates risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations are investigated. The review includes identifying and documenting the controls in place to address the CUECs.	Inspected the vendor risk assessment matrix documentation and determined that the company valuated risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations were investigated. Inspected the infrastructure provider SOC 2 report review and determined that it included identifying and documenting the controls in place at to address the CUECs.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
131	Access to system resources is protected through a combination of firewalls, VPNs, native operating	Inspected the system architecture diagram and determined that access was protected through a	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	system access controls, database management system security, application controls and intrusion detection monitoring software.	combination of firewalls, VPNs, native operating system security, database management system security and application controls.	
78	Anti-malware software is installed on workstations, laptops, and servers supporting such software. The anti-malware software is configured to periodically receive updated virus signatures.	Inspected the anti-malware dashboard status for employees' workstations, laptops, and servers and determined that anti-malware software was installed on workstations, laptops, and servers supporting such software. The anti-malware software was configured to periodically receive updated virus signatures.	No deviations noted.
87	A network firewall is configured and operating on production environments to prevent malicious network access to networks and machines.	Inspected the firewall configuration and determined that network firewall was configured and operated on production environments to prevent malicious network access to networks and machines.	No deviations noted.
43	Server disks residing in production environments, including backups, are encrypted at rest.	Inspected the encryption configuration and determined that server disks residing in production environments, including backups, were encrypted at rest.	No deviations noted.
54	Buckets residing in production environments, including backups, are encrypted at rest.	Inspected the encryption configuration and determined that buckets residing in the production environments, including backups, were encrypted at rest.	No deviations noted.

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
33	Production environment access permissions are restricted to authorized users only. Specific developers can be granted temporary access for specific projects. The access is logged and reviewed.	Inspected the list of users with access to the production and database environments and determined that specific developers can be granted access to specific projects. Inspected a sample of access requests to the production and database environments and determined that	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		specific developers can be granted temporary access for specific projects. Inspected the log review documentation and determined that access and changes within the production are logged and reviewed	
34	Sensitive SaaS application access permissions are restricted to authorized users only, for the source control, build, and identity management tools.	Inspected the list of users with access to the sensitive SaaS application and determined that sensitive SaaS application access permissions were restricted to authorized users only, for source control, build, and identity management tools.	No deviations noted.
75	Direct remote access to production servers is restricted and performed through a dedicated jump server (bastion host) or VPN.	Inspected the production access configurations from AWS and determined that remote access to production servers was restricted and performed through a dedicated jump server (bastion host) or VPN.	No deviations noted.
131	Access to system resources is protected through a combination of firewalls, VPNs, native operating system access controls, database management system security, application controls and intrusion detection monitoring software.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls.	No deviations noted.
32	Databases residing in production environments, including backups, are encrypted at rest.	Inspected the encryption configuration and determined that databases residing in production environments, including backups, were encrypted at rest.	No deviations noted.
78	Anti-malware software is installed on workstations, laptops, and servers supporting such software. The anti-malware software is configured to periodically receive updated virus signatures.	Inspected the anti-malware dashboard status for employees' workstations, laptops, and servers and determined that anti-malware software was installed on workstations, laptops, and servers supporting such software. The anti-malware software was configured to periodically receive updated virus signatures.	No deviations noted.
93	Customer and user passwords are encrypted or hashed, either in storage or by using a third-party	Inspected customer and user passwords configuration and determined that customer and user passwords were encrypted or hashed in database.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	user management tool that complies with this requirement.		

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
78	Anti-malware software is installed on workstations, laptops, and servers supporting such software. The anti-malware software is configured to periodically receive updated virus signatures.	Inspected the anti-malware dashboard status for employees' workstations, laptops, and servers and determined that anti-malware software was installed on workstations, laptops, and servers supporting such software. The anti-malware software was configured to periodically receive updated virus signatures.	No deviations noted.
6	The company evaluates risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations are investigated. The review includes identifying and documenting the controls in place to address the CUECs.	Inspected the vendor risk assessment matrix documentation and determined that the company valuated risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations were investigated. Inspected the infrastructure provider SOC 2 report review and determined that it included identifying and documenting the controls in place at to address the CUECs.	No deviations noted.
74	Device storage, including laptops and workstations, is encrypted by automatic software to restrict access to sensitive information.	Inspected the devices tool dashboard and configuration and determined that the device storage, including for laptops and workstations, were encrypted by automatic software to restrict access to sensitive information.	No deviations noted.
116	Penetration tests are performed on products on an annual basis and high and critical issues are documented, tracked, investigated and resolved.	Inspected the penetration test report and determined that penetration tests were performed on products on an annual basis. High and critical issues were documented, tracked, investigated and resolved.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
111	User log activity auditing and audit trail for database, servers, and applications is performed and reviewed at least annually.	Inspected a sample of access logs to production, DB, backup, and application and determined that user log activity auditing and audit trail for database, servers, and applications was performed. Inspected a sample of audit alerts and determined that the logs were reviewed at least annually.	No deviations noted.
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients.	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were notified of events related to the security, availability, or confidentiality of service to clients.	No deviations noted.
116	Penetration tests are performed on products on an annual basis and high and critical issues are documented, tracked, investigated and resolved.	Inspected the penetration test report and determined that penetration tests were performed on products on an annual basis. High and critical issues were documented, tracked, investigated and resolved.	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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
78	Anti-malware software is installed on workstations, laptops, and servers supporting such software. The	Inspected the anti-malware dashboard status for employees' workstations, laptops, and servers and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	anti-malware software is configured to periodically receive updated virus signatures.	determined that anti-malware software was installed on workstations, laptops, and servers supporting such software. The anti-malware software was configured to periodically receive updated virus signatures.	
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients.	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were notified of events related to the security, availability, or confidentiality of service to clients.	No deviations noted.
74	Device storage, including laptops and workstations, is encrypted by automatic software to restrict access to sensitive information.	Inspected the devices tool dashboard and configuration and determined that the device storage, including for laptops and workstations, were encrypted by automatic software to restrict access to sensitive information.	No deviations noted.
116	Penetration tests are performed on products on an annual basis and high and critical issues are documented, tracked, investigated and resolved.	Inspected the penetration test report and determined that penetration tests were performed on products on an annual basis. High and critical issues were documented, tracked, investigated and resolved.	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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	related to the security, availability, or confidentiality of service to clients.	everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were notified of events related to the security, availability, or confidentiality of service to clients.	

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.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	Service interruptions, maintenance and updates are communicated to customers through emails, status page links, chat or other means of communication.	Inspected the company's status page and determined that service interruptions, maintenance and updates were communicated to customers through a status page link. No service interruption occurred during the audit period.	No deviations noted.
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients.	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were notified of events related to the security, availability, or confidentiality of service to clients.	No deviations noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	Service interruptions, maintenance and updates are communicated to customers through emails, status page links, chat or other means of communication.	Inspected the company's status page and determined that service interruptions, maintenance and updates were communicated to customers through a status page link. No service interruption occurred during the audit period.	No deviations noted.
26	Database backup restoration tests are performed to validate the effectiveness of the automated database backup process.	Inspected the restore test documentation and determined that the database backup restoration tests were performed to validate the effectiveness of the automated database backup process.	No deviations noted.

Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
60	Permissions for development tools, including source control and CI/CD, are restricted to authorized users only.	Inspected the list of users with access to development tools, including source control and CI\CD tools and determined that permissions were restricted to authorized users only.	No deviations noted.
67	Permissions for approving merge requests are restricted to authorized personnel.	Inspected the list of users with permission to approve merge requests and determined that it was restricted to authorized personnel.	No deviations noted.
59	Changes in software are documented and prioritized using a change management tool and assigned to the relevant stakeholder. Each code change in the source control tool should be linked to the ticket documenting that change and vice versa. Changes are documented and prioritized using agreed communication channels.	For a sample of changes, inspected the change management tickets and determined that changes in software were documented and prioritized using a change management tool and assigned to the relevant stakeholder. Each code change in the source control tool linked to the ticket documenting that change and vice versa. Changes were documented and prioritized using agreed communication channels.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
61	Code changes are reviewed along with the pull request and approved by professional authorized users before being merged to production. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment.	For a sample of changes, inspected the code review that was performed and determined that code changes were reviewed along with the pull request and approved by authorized users before being merged to production. Inspected the branch protected role configuration and determined that the code review was mandatory in order to continue in the SDLC process and deploy a version to the production environment.	No deviations noted.
69	Testing procedures including unit testing and end-to-end testing are in place, automatically or manually.	For a sample of changes, inspected the test procedures and the results and determined that testing procedures including unit testing and end-to-end testing were in place, automatically or manually.	No deviations noted.
77	Automated source code vulnerability scans are performed for each merge to default branches in an attempt to identify and fix security-related weaknesses (flaws) in the code.	For a sample of changes, inspected the documentation of the vulnerability scans performed and determined that automated source code vulnerability scans were performed for merged to default branches in an attempt to identify and fix security-related weaknesses (flaws) in the code.	No deviations noted.
137	Infrastructure changes are documented, prioritized and tracked. Changes are approved by authorized personnel.	For a sample of Infrastructure changes, inspected the change management tickets and determined that they were documented, prioritized and tracked. Changes were approved by authorized personnel.	No deviations noted.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	Vendor risk management policy is documented, and the policy defines how the company evaluates, engages, and provisions new and existing vendors.	Inspected the company's vendor risk management policy and determined that a vendor risk management policy was documented and the policy defines how the	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		company evaluated, engaged, and provisioned new and existing vendors.	
6	The company evaluates risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations are investigated. The review includes identifying and documenting the controls in place to address the CUECs.	Inspected the vendor risk assessment matrix documentation and determined that the company valuated risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations were investigated. Inspected the infrastructure provider SOC 2 report review and determined that it included identifying and documenting the controls in place at to address the CUECs.	No deviations noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that the board met at least on a quarterly basis, documented and had a fixed agenda. Meeting minutes were retained.	No deviations noted.
22	Management meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected the management meeting minutes and invitations and determined that the management of the company met on a quarterly basis to discuss ongoing issues and updates. Meeting minutes were retained.	No deviations noted.
23	Prior to engaging with third-party vendors an NDA must be signed.	Inspected a sample of signed NDA's and determined that prior to engaging with third-party vendors an NDA was signed.	No deviations noted.
5	Vendor risk management policy is documented, and the policy defines how the company evaluates, engages, and provisions new and existing vendors.	Inspected the company's vendor risk management policy and determined that a vendor risk management policy was documented and the policy defines how the	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		company evaluated, engaged, and provisioned new and existing vendors.	
6	The company evaluates risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations are investigated. The review includes identifying and documenting the controls in place to address the CUECs.	Inspected the vendor risk assessment matrix documentation and determined that the company valuated risks regarding vendors, partners, subcontractors, infrastructure providers and other related third parties, including review of the security compliance reports. Deviations were investigated. Inspected the infrastructure provider SOC 2 report review and determined that it included identifying and documenting the controls in place at to address the CUECs.	No deviations noted.
10	Risk assessment meetings where stakeholders evaluate risks and threats take place and documented.	Inspected the risk assessment meeting invitations and minutes and determined that a risk assessment meeting took place on an annual basis and was documented.	No deviations noted.
11	Risk assessment that follows the organization's policy is performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations.	Inspected the risk assessment matrix documentation and determined that risk assessment that followed the organization's policy was performed and documented to analyze, identify, evaluate and address internal and external risks. Also, risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupted business operations.	No deviations noted.

Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	Service interruptions, maintenance and updates are communicated to customers through emails, status page links, chat or other means of communication.	Inspected the company's status page and determined that service interruptions, maintenance and updates were communicated to customers through status page link. No service interruption occurred during the audit period.	No deviations noted.
25	Production databases are located in more than one availability zone to ensure high availability.	Inspected the availability zones configuration from AWS and determined that production databases were located in more than one availability zone to ensure high availability.	No deviations noted.
27	Production databases are automatically backed up in high granularity.	Inspected the AWS database backup configuration and determined that production databases were automatically backed up in high granularity.	No deviations noted.
113	Infrastructure monitoring tools are in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Key Trustmi personnel is notified of events related to the security, availability, or confidentiality of service to clients.	Inspected the monitoring configuration and determined that infrastructure monitoring tools were in place to gather metrics about the operations of an IT environment hardware and software to ensure everything functions as expected to support applications and services. Inspected the alert configuration and a sample of alerts and determined that key Trustmi personnel were notified of events related to the security, availability, or confidentiality of service to clients.	No deviations noted.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
13	Service interruptions, maintenance and updates are communicated to customers through emails, status page links, chat or other means of communication.	Inspected the company's status page and determined that service interruptions, maintenance and updates were communicated to customers through a status page link. No service interruption occurred during the audit period.	No deviations noted.
25	Production databases are located in more than one availability zone to ensure high availability.	Inspected the availability zones configuration from AWS and determined that production databases were located in more than one availability zone to ensure high availability.	No deviations noted.
27	Production databases are automatically backed up in high granularity.	Inspected the AWS database backup configuration and determined that production databases were automatically backed up in high granularity.	No deviations noted.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
26	Database backup restoration tests are performed to validate the effectiveness of the automated database backup process.	Inspected the restore test documentation and determined that the database backup restoration tests were performed to validate the effectiveness of the automated database backup process.	No deviations noted.
28	Backup and disaster recovery plan policy is documented, reviewed, and tested periodically. The policy defines the company's data backup and disaster recovery directions to ensure the company keeps providing required services in case of a disaster.	Inspected the backup and disaster recovery plan and determined that backup and disaster recovery plan policy was documented, reviewed, and tested periodically. The policy defined the company's data backup and disaster recovery directions to ensure the company kept providing required services in case of a disaster.	No deviations noted.

Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	Board of directors' meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that the board met at least on a quarterly basis, documented and had a fixed agenda. Meeting minutes were retained.	No deviations noted.
22	Management meetings are held on a quarterly basis, documented and have a fixed agenda. Meeting minutes are retained.	Inspected the management meeting minutes and invitations and determined that the management of the company met on a quarterly basis to discuss ongoing issues and updates. Meeting minutes were retained.	No deviations noted.
23	Prior to engaging with third-party vendors an NDA must be signed.	Inspected a sample of signed NDA's and determined that prior to engaging with third-party vendors an NDA was signed.	No deviations noted.
51	Internal employees sign on an NDA as part of their employment contract with the Company.	For a sample of new employees, inspected the signed NDA's and determined that internal employees signed on an NDA as part of their employment contract with the company.	No deviations noted.
32	Databases residing in production environments, including backups, are encrypted at rest.	Inspected the encryption configuration and determined that databases residing in production environments, including backups, were encrypted at rest.	No deviations noted.
111	User log activity auditing and audit trail for database, servers, and applications is performed and reviewed at least annually.	Inspected a sample of access logs to production, DB, backup, and application and determined that user log activity auditing and audit trail for database, servers, and applications was performed. Inspected a sample of audit alerts and determined that the logs were reviewed at least annually.	No deviations noted.
74	Device storage, including laptops and workstations, is encrypted by automatic software to restrict access to sensitive information.	Inspected the devices tool dashboard and configuration and determined that the device storage, including for laptops and workstations, were encrypted by automatic software to restrict access to sensitive information.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies.	No deviations noted.

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
23	Prior to engaging with third-party vendors an NDA must be signed.	Inspected a sample of signed NDA's and determined that prior to engaging with third-party vendors an NDA was signed.	No deviations noted.

Privacy

P1.0: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
101	An up-to-date privacy policy is available on the company's website and reviewed and updated by management. The policy outlines how the company handles private data and fully discloses the types of information the company may collect via its products and website, as well as how it may use this information.	Inspected the privacy policy and website and determined that an up-to-date privacy policy was available on the company's website and was reviewed and updated by management. The policy outlined how the company handles private data and fully discloses the types of information the company may collect via its products and website, as well as how it may use this information.	No deviations noted.
102	The company conducts an annual privacy awareness training program to maintain privacy awareness posture.	Inspected the privacy awareness training meeting invitations and the training materials and determined that the company conducted an annual privacy	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		awareness training program to maintain privacy awareness posture.	
107	Privacy statements informing customers of the types of collected data and how this data is used are provided in the company's website and application and reviewed periodically.	Inspected the privacy policy and website and determined that a privacy statement was available online for customers and reviewed periodically.	No deviations noted.

P2.0: Privacy Criteria Related to Choice and Consent

P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
107	Privacy statements informing customers of the types of collected data and how this data is used are provided in the company's website and application and reviewed periodically.	Inspected the privacy policy and website and determined that a privacy statement was available online for customers and reviewed periodically.	No deviations noted.

P3.0: Privacy Criteria Related to Collection

P3.1: Personal information is collected consistent with the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
100	The collection and processing of personal information is consistent with the company's privacy commitments and system requirements.	Inspected the privacy policy, terms of use, contracts, and website and determined that personal information was collected in consistence with the company's objectives related to privacy. The collection and processing of personal information was consistent with the company's privacy commitments and system requirements.	No deviations noted.

P3.2: For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
97	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the Company's privacy policies. The names of such a person or group and their responsibilities are defined.	Inspected the company's set of policies and procedures determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies.	No deviations noted.

P4.0: Privacy Criteria Related to Use, Retention, and Disposal

P4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
109	Access to personal information in databases is restricted to authorized Company's personnel.	Inspected the password policies, user access lists and the user access reviews and determined that access to personal information in databases was restricted to authorized Company's personnel.	No deviations noted.

P4.2: The entity retains personal information consistent with the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
99	The company securely disposes of personal information to meet the entity's objectives related to privacy.	Inspected the user account deletion procedure and determined that the company securely disposes of personal information to meet the entity's objectives related to privacy.	No deviations noted.
132	The company securely retains personal information to meet the entity's objectives related to privacy.	Inspected a sample of customer private data deletion logs and determined that the company securely retained personal information to meet the entity's objectives related to privacy.	No deviations noted.

P4.3: The entity securely disposes of personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
99	The company securely disposes of personal information to meet the entity's objectives related to privacy.	Inspected the user account deletion procedure and determined that the company securely disposes of personal information to meet the entity's objectives related to privacy.	No deviations noted.

P5.0: Privacy Criteria Related to Access

P5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
103	The company grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	Inspected a sample of data subject access requests and the company privacy policy and determined that the company granted identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provided physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access was denied, data subjects were informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	No deviations noted.
104	Third parties requiring access to company's private data provide privacy obligations through privacy standards or signed contracts. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	Inspected the company's data processing agreements with vendors and sub-processors list and determined that third parties' requiring access to company's private data provided privacy obligations through privacy standards or signed contracts. The entity assessed those parties' compliance on a periodic and as-needed basis and took corrective action, if necessary.	No deviations noted.

P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
105	The company grants identified and authenticated data subjects the ability to opt-out and to erase their stored data in the company's applications.	Inspected a sample of data subject access requests and the company privacy policy and determined that the company granted identified and authenticated data subjects the ability to opt-out and to erase their stored data in the company's applications.	No deviations noted.

P6.0: Privacy Criteria Related to Disclosure and Notification

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
136	The company creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	Inspected the incident response and data breach policy and determined that the company created and retained a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	No deviations noted.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
136	The company creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	Inspected the incident response and data breach policy and determined that the company created and retained a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	No deviations noted.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
136	The company creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	Inspected the incident response and data breach policy and determined that the company created and retained a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	No deviations noted.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
133	The company corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Inspected the privacy policy and determined the company corrected, amended, or appended personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction was denied, data subjects were informed of the denial and reason for such denial to meet the entity's objectives related to privacy. There was no right to access requests in the audit period.	No deviations noted.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
133	The company corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for	Inspected the privacy policy and determined the company corrected, amended, or appended personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	objectives related to privacy. If a request for correction was denied, data subjects were informed of the denial and reason for such denial to meet the entity's objectives related to privacy. There was no right to access requests in the audit period.	

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
133	The company corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Inspected the privacy policy and determined the company corrected, amended, or appended personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction was denied, data subjects were informed of the denial and reason for such denial to meet the entity's objectives related to privacy. There was no right to access requests in the audit period.	No deviations noted.

P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
134	The company provides notification of data (including personal data) breaches and incidents, to the affected data subjects, regulators, and others.	Inspected the incident response and data breach policy and determined that the company provided notification of data (including personal data) breaches and incidents, to the affected data subjects, regulators, and others.	No deviations noted.

P7.0: Privacy Criteria Related to Quality

P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
95	Customer contracts include privacy considerations on which the customer signs and acknowledge how its personal data is collected and used.	Inspected a sample of customer contracts and terms of service and determined that customer contracts included privacy considerations on which the customer signs and acknowledged how their personal data was collected and used.	No deviations noted.

P8.0: Privacy Criteria Related to Monitoring and Enforcement

P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
135	The company implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	Inspected the privacy policy and determined that the company implemented a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies were made or taken in a timely manner.	No deviations noted.

****