Interface, Inc.

System and Organization Controls (SOC 2) Type II Report

Description of Literal AI Application relevant to the Trust Services Criteria of Security

October 1, 2024 through December 31, 2024

STATEMENT OF CONFIDENTIALITY

This report, including the Description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's system related to Interface Application relevant to the Security during some or all of the period October 1, 2024 through December 31, 2024, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties. Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.s

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITORS' REPORT

1 INDEPENDENT SERVICE AUDITORS' REPORT

To the management of Interface, Inc.

Scope

We have examined the description of the system provided by Management of Interface, Inc., (the "Service Organization" or "Interface") included fin Section 3, "Description of Systems Provided by Service Organization" of its Interface application throughout the period October 1, 2024 to December 31, 2024 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period October 1, 2024 to December 31, 2024, to provide reasonable assurance that Interface's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Interface uses Amazon Web Services, Inc., (AWS) ("subservice organization"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Interface, to achieve Interface's service commitments and system requirements based on the applicable trust services criteria. The Description presents Interface's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Interface's controls. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Management of Interface 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 Interface service commitments and system requirements would be achieved. Management of Interface has provided the accompanying assertion in Section 2 titled, "Management Assertion Provided by Interface, Inc." (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Management of Interface is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and operating effectiveness of controls stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the Interface's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a Description of a service organization's system and the suitability of the design 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 did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that Interface achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the Description.

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and therefore may not include every aspect of the system that each individual report user may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system

requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4, "Information Provided by the Service auditor: Test of controls".

Opinion

In our opinion, in all material respects:

a) The Description presents Interface's system that was designed and implemented throughout the period October 1, 2024 to December 31, 2024, in accordance with the description criteria.

b) The controls stated in the Description were suitably designed throughout the period October 1, 2024 to December 31, 2024, to provide reasonable assurance that Interface'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 Interface's controls throughout that period.

c) The controls stated in the Description operated effectively throughout the period October 1, 2024 to December 31, 2024, to provide reasonable assurance that Interface's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of Interface's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Interface, user entities of Interface application during some or all of the period October 1, 2024 to December 31, 2024, business partners of Interface subject to risks arising from interactions with the Interface's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by Interface.
- How Interface's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at Interface's to achieve Interface's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use Interface's services.

- The applicable trust services criteria.
- The risks that may threaten the achievement of Interface'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.

Accorp Partners CPA LLC

ACCORP PARTNERS CPA LLC
License No.: PAC-FIRM-LIC-47383
Date: February 25, 2025

SECTION 2

MANAGEMENT'S ASSERTION PROVIDED BY SERVICE ORGANIZATION

MANAGEMENT ASSERTION PROVIDED BY INTERFACE, INC.

For the period from October 1, 2024 through December 31, 2024

We have prepared the accompanying System Description Provided by Service Organization (Description) of Interface, Inc. (the "Service Organization" or "Interface") 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 Literal AI application (System) that may be useful when assessing the risks arising from interactions with the System throughout the period October 1, 2024 to December 31, 2024, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Interface uses Amazon Web Services, Inc. (AWS) ("subservice organization"). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Interface , to achieve Interface's service commitments and system requirements based on the applicable trust services criteria. The description presents Interface's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Interface controls. The description does not disclose the actual controls at the subservice organization. The description does not extend to controls of the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Interface, to achieve Interface's service commitments and system requirements based on the applicable trust services criteria. The description presents Interface's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Interface's controls. The description does not extend to controls of the user entities.

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

a. The description presents the System that was designed and implemented throughout the period October 1, 2024 to December 31, 2024 in accordance with the description Criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2024 to December 31, 2024, to provide reasonable assurance that Interface'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 organizations and user entities applied the complementary controls assumed in the design of Interface's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2024 to December 31, 2024, to provide reasonable assurance that Interface's service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organizations and user

entities applied the complementary controls assumed in the design of Interface's controls operated effectively throughout that period.

For Interface, Inc.

Name: Aymeric Beaumet

Title: CTO

Date: Feb 25th, 2025

SECTION 3
DESCRIPTION OF THE SYSTEM

3 DESCRIPTION OF SYSTEMS PROVIDED BY SERVICE ORGANIZATIONS

3.1 Overview of Service Organization and Services Provided

Interface, Inc. is a company dedicated to developing key components that integrate Artificial General Intelligence (AGI) into daily life. Their mission is to enhance productivity by leveraging AI to manage and optimize conversations, aiming to give back an hour to busy individuals.

The company's approach involves creating:

- Communication platforms that provide AI with necessary context and memory.
- Action models that interpret conversational context to perform tasks on behalf of users.
- Retrieval tools that accurately recall information.
- Elegant interfaces that seamlessly integrate these components.

3.2 Principal Service Commitments and System Requirements

Interface designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Interface makes to customers and the compliance requirements that Interface has established for their services.

Security commitments to user entities are documented and communicated in Interface's customer agreements, as well as in the description of the service offering provided online. Interface's security commitments are standardized and based on some common principles.

These principles include but are not limited to, the following:

- The fundamental design of Interface's Interface application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role;
- Interface implements various procedures and processes to control access to the production environment and the supporting infrastructure; and
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

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

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Interface and user entities.

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

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans are tested on a periodic basis; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Interface establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Interface's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how staff is hired

3.3 Components of the System used to provide services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

Infrastructure and Network Architecture

The production infrastructure for the Interface, Inc software application is hosted on Amazon Web Services (AWS) in their various regions across eu-west-1.

Interface application uses a virtual and secure network environment on top of AWS infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. Interface application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the AWS Internet Gateway, over to a Virtual Private Cloud that

1. Houses the entire application runtime
2. Protects the application runtime from any external networks

The internal networks of AWS are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

Software

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

System/ Application	Business Function / Description
Interface Application	Access to the application is through a web/mobile interface and user authentication.
AWS IAM	Identity and access management console for AWS resources.
AWS Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.
GitHub App	Source code repository, version control system, and build software.
Google Workspace	Identity/Email provider for all Interface employees

Supporting Tools	Business Function / Description
Go, Postgresql, Valkey	Programming Language used for Interface application
Google Workspace	Office communication services

People

Interface's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Data

Data, as defined by Interface, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports.
- Input reports.
- System files
- Error logs

All data that is managed, processed, and stored as a part of the Interface Application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization. All data is assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer	Highly valuable and sensitive information	• Customer system and

Data Sensitivity	Description	Examples
confidential	where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally, or was entrusted to Interface by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Interface's PII • Unpublished financial Information • Documents and processes explicitly marked as confidential • Unpublished goals, forecasts, and initiatives marked as confidential • Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	Public website Press releases

All customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data backup policy.

Procedures and Policies

Formal policies and procedures have been established to support the Interface application. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

Interface also provides information to clients and staff members on how to report failures,

incidents, concerns, or complaints related to the services or systems provided by the Interface application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

3.4 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and implementation of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Interface's description of the system. This section provides information about the five interrelated components of internal control at Interface, including:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring controls

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Interface's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Interface's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Interface and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization’s values and behavioral standards to staff members
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Interface's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

Interface's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information.

Interface's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

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

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.

Organizational Structure and Assignment of Authority and Responsibility

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

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources

Interface's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the

management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

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

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

Interface's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Interface identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Interface application, and the management has implemented various measures designed to manage these risks.

Interface believes that effective risk management is based on the following principles:

- Senior management's commitment to the security of Interface application
- The involvement, cooperation, and insight of all Interface staff
- Initiating risk assessments with discovery and identification of risks
- A thorough analysis of identified risks
- Commitment to the strategy and treatment of identified risks
- Communicating all identified risks to the senior management
- Encouraging all Interface staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Interface application. The Interface risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Interface's Information Security Officer and the department or individuals responsible for the area being assessed. All Interface staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

Interface uses a number of vendors to meet its business objectives. Interface understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Interface employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Interface assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Interface's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Interface management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Interface identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Interface's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Information and Communication

Interface maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, Interface also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Monitoring Controls

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

Control Activities

Interface's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Significant Events and Conditions

Interface has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the software application.

Physical Security

The in-scope system and supporting infrastructure are hosted by AWS. As such, AWS is responsible for the physical security controls of the in-scope system. Interface reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Interface application.

Logical Access Control

The Interface Application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

Interface has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary. Access to critical systems requires multi-factor authentication (MFA) wherever possible. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Interface customer data. Staff is encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special-character based. Password configuration settings are configured on each critical system. Additionally, company-owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Change Management

A documented Change Management policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Interface system are reviewed, deployed, and managed. The policy covers all changes made to the Interface application, regardless of their size, scope, or potential impact.

The change management policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Interface Application can be initiated by a staff member with an appropriate role. Interface uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Incident Management

Interface has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Interface via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- Low severity incidents are those that do not require immediate remediation. These typically include a partial service of Interface being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- Medium severity incidents are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- High severity incidents are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.

- Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post- mortems may include updates to the security program or changes to systems required as a result of incidents.

Cryptography

User requests to Interface's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Interface web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Interface uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk- ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that includes policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/ workstations.

Availability

Interface has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Boundaries of the System

The scope of this report includes the Interface application. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

Interface depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management

understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

3.5 Complementary User Entity Controls

Interface's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Interface customers.

For customers to rely on the information processed through the Interface's Interface application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- Customers are responsible for managing their organization's Interface application account as well as establishing any customized security solutions or automated processes through the use of setup features
- Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Interface application account
- Customers are responsible for notifying Interface of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Interface application.
- Customers are responsible for any changes made to user and organization data stored within the Interface application.
- Customers are responsible for communicating relevant security and availability issues and incidents to Interface through identified channels.

3.6 Complementary Subservice Organization Controls

Controls at Service organization and controls at User organization related to Interface Application to its customers relevant to the Security ("in-scope trust service criteria"), cover only a portion of the overall internal control structure of its clients. The control objectives cannot be achieved without taking into consideration operating effectiveness of controls at subservice organization providing services to service organization to perform services provided to user entity that are likely to be relevant to those user entity internal control over financial reporting.

This section highlights those internal control structure responsibilities, Interface believes should be present at all applicable subservice organization, and which Interface has considered in developing its control structure policies and the procedures described in this report.

The subservice organization used by Interface relevant to providing services related to Interface is shown below:

Subservice Organization	Service Provided
Amazon Web Services Inc. (AWS)	Cloud computing services

Activity Expected to be Implemented by Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	CC6.4, A1.2
Encryption methods are used to protect data in transit and at rest.	CC6.1
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	A1.2
A defined Data Classification Policy specifies classification levels and control requirements to meet the company's commitments related to confidentiality.	C1.1
A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.	C1.2

3.7 Trust services criteria and Description of Related Controls:

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
Control Environment			
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	BT-01	Material violations of the company's Acceptable Use Policy, Code of Conduct, and Information Security policies and procedures applicable to each employee subjects the individual to disciplinary action that could include termination.
		BT-02	Organizational values and behavioral standards are communicated to all personnel through an Employee Handbook, which outlines the company's policy regarding Standards of Conduct and Code of Business Ethics.
		BT-03	Company employees are required to sign and attest their adherence to applicable company policies and procedures.
		BT-04	All employees and contractors must sign a confidentiality agreement with the company prior to gaining access to any sensitive information.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
		BT-05	Background checks are performed on newly hired employees where permitted by law.
		BT-06	The Acceptable Use Policy outlines the acceptable use of computer equipment and systems at the company.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	BT-07	The company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.
		BT-08	A Board of Directors exercises independent oversight of the company's strategic direction, operational performance, and internal control.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	BT-09	The company has an appropriate organizational structure based on functional departments, with an executive leader heading each department.
		BT-10	Management and the Board of Directors consider requirements relevant to security, availability, processing integrity, and confidentiality. These considerations are documented in the company's Information Security Policy, which specifically delegates the overall responsibility of security to the Security Officer.
		BT-11	Roles and responsibilities of company employees are communicated through documented job descriptions.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	BT-12	The company has established a formal review process that includes semi-annual employee self-reviews and immediate manager reviews. Reviews include performance assessments, goal setting, and an evaluation of resources required for the next review period.
		BT-13	Security awareness training is provided to new employees, and to all employees on a recurring annual basis, to promote strong security practices for the whole company.
		BT-11	Roles and responsibilities of company employees are communicated through documented job descriptions.
		BT-05	Background checks are performed on newly hired employees where permitted by law.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
CC 1.5	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	BT-07	The company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.
		BT-01	Material violations of the company's Acceptable Use Policy, Code of Conduct, and Information Security policies and procedures applicable to each employee subjects the individual to disciplinary action that could include termination.
		BT-12	The company has established a formal review process that includes semi-annual employee self-reviews and immediate manager reviews. Reviews include performance assessments, goal setting, and an evaluation of resources required for the next review period.
		BT-11	Roles and responsibilities of company employees are communicated through documented job descriptions.
Communication and Information			
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.
		BT-15	The company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.
		BT-16	Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.
		BT-17	Security tools are deployed and system components are configured to monitor for security-related events.
		BT-18	A static code analysis tool is configured to scan the source code for vulnerabilities.
		BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
		BT-20	All company and customer data is classified as per the data classification policy.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	BT-21	Employees have access to an internal support channel that can be used to report incidents, concerns, and complaints.
		BT-15	The company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.
		BT-13	Security awareness training is provided to new employees, and to all employees on a recurring annual basis, to promote strong security practices for the whole company.
		BT-11	Roles and responsibilities of company employees are communicated through documented job descriptions.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	BT-22	The company's Privacy Policy is available online to visitors and customers, and outlines the receipt, sharing, use, and disposal of visitor and subscriber data.
		BT-23	The company communicates system changes to its users and customers through an established channel and procedure.
		BT-24	The company maintains a customer-accessible technical documentation site containing high-level overviews and detailed information about the company's products and services, including security-oriented articles and guides.
		BT-25	External users are provided with a support channel for reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.
		BT-26	The company's Terms of Use are available online to visitors and customers, and outline the requirements and commitments of both parties relative to security and confidentiality.
Risk Assessment			
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification	BT-27	The company maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
	and assessment of risks relating to objectives.		
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.	BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.
		BT-28	The company maintains an inventory of IT infrastructure devices.
		BT-29	The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.
		BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	BT-30	The company assesses the potential for fraud from internal or external stakeholders as part of its Risk Assessment process.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	BT-31	Vendors are evaluated on a periodic basis, by reviewing their audit reports or other means, in order to track and determine the impact of any changes in their security posture.
		BT-29	The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.
Monitoring Activities			
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	BT-07	The company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.
		BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
		BT-16	Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.
		BT-17	Security tools are deployed and system components are configured to monitor for security-related events.
		BT-18	A static code analysis tool is configured to scan the source code for vulnerabilities.
		BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	BT-07	The company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.
Control Activities			
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	BT-32	The company designs and implements controls to mitigate risks identified during the risk assessment process.
		BT-33	Management periodically reviews control activities to reaffirm each control's relevance, and updates the set of controls as necessary.
		BT-15	The company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.
		BT-29	The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support	BT-32	The company designs and implements controls to mitigate risks identified during the risk assessment process.
		BT-33	Management periodically reviews control activities to reaffirm each control's

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
	the achievement of objectives.		relevance, and updates the set of controls as necessary.
		BT-34	Control activities over the technology infrastructure and technology access control are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
		BT-29	The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	BT-01	Material violations of the company's Acceptable Use Policy, Code of Conduct, and Information Security policies and procedures applicable to each employee subjects the individual to disciplinary action that could include termination.
		BT-15	The company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.
		BT-35	Control owners take corrective actions when issues and nonconformities with their controls are identified.
		BT-20	All company and customer data is classified as per the data classification policy.
Logical and Physical Access Controls			
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	BT-36	The company leverages SSO authentication for sensitive systems, wherever available.
		BT-37	All users with privileged access to sensitive systems are required to use a password management solution.
		BT-38	Access to sensitive systems and resources is granted based on the principle of least privilege.
		BT-39	The company maintains an inventory of all information systems, services, and assets, and classifies them based on the data they store. Inventory is reviewed as part of an annual Risk Assessment.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
		BT-40	Defined permission roles are utilized to assign and segregate access privileges to data and systems.
		BT-41	Administrative access privileges for sensitive systems are only granted to a restricted, small set of personnel, with a clearly defined business need to maintain and administer those systems.
		BT-28	The company maintains an inventory of IT infrastructure devices.
		BT-42	Access to sensitive systems requires multi-factor authentication.
		BT-43	Password configuration settings are managed in compliance with the company's Password Policy.
		BT-44	The company maintains documented guidance on the selection and configuration of appropriate cryptographic methods.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	BT-45	Termination checklists are executed upon separation with an employee or contractor to ensure asset return, and prompt and complete access revocation.
		BT-38	Access to sensitive systems and resources is granted based on the principle of least privilege.
		BT-46	Access to systems is requested by filing an internal access request ticket specifying the need for the access. Access is approved by the respective manager and granted by administrators based on a least-privilege principle.
		BT-43	Password configuration settings are managed in compliance with the company's Password Policy.
		BT-47	A review of users with access to Customer Confidential systems is performed periodically to ensure that access is restricted to appropriate personnel.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving	BT-45	Termination checklists are executed upon separation with an employee or contractor to ensure asset return, and prompt and complete access revocation.
		BT-40	Defined permission roles are utilized to assign and segregate access privileges to data and systems.
		BT-46	Access to systems is requested by filing an internal access request ticket specifying

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
	consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		the need for the access. Access is approved by the respective manager and granted by administrators based on a least-privilege principle.
		BT-41	Administrative access privileges for sensitive systems are only granted to a restricted, small set of personnel, with a clearly defined business need to maintain and administer those systems.
		BT-43	Password configuration settings are managed in compliance with the company's Password Policy.
		BT-47	A review of users with access to Customer Confidential systems is performed periodically to ensure that access is restricted to appropriate personnel.
CC 6.4	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.		Not applicable as the application and infrastructure is hosted by cloud service provider.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	BT-49	Customer data is securely disposed of after its retention period passes, and any retained data is sanitized and anonymized.
		BT-50	Retention periods for customer data are specified in the company's Data Retention Procedure and adhere to compliance, regulatory, contractual, and organizational requirements.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.
		BT-51	Firewalls are configured to restrict network traffic to the minimum required for the system to function.
		BT-52	TLS usage is evaluated on a quarterly basis using tools such as ssllabs and any

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
			grades lower than A are promptly corrected.
		BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.
		BT-44	The company maintains documented guidance on the selection and configuration of appropriate cryptographic methods.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	BT-51	Firewalls are configured to restrict network traffic to the minimum required for the system to function.
		BT-53	Data stores are configured to enable encryption at rest.
		BT-52	TLS usage is evaluated on a quarterly basis using tools such as ssllabs and any grades lower than A are promptly corrected.
		BT-54	Data in transit over the public Internet is encrypted with industry-standard algorithms.
		BT-55	Third-party cloud filestores such as S3 and GCS are configured with a minimum server-side encryption using the vendor's key.
		BT-44	The company maintains documented guidance on the selection and configuration of appropriate cryptographic methods.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	BT-56	The company monitors the IT infrastructure devices for compliance with the Asset Management Policy and checks for requirements such as hard drive encryption, user authentication requirements, and security patching.
		BT-57	OS patches and docker image updates are applied at least weekly.
		BT-06	The Acceptable Use Policy outlines the acceptable use of computer equipment and systems at the company.
System Operations			
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures	BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
	to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		resolved and the rest are prioritized as appropriate.
		BT-18	A static code analysis tool is configured to scan the source code for vulnerabilities.
		BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.
		BT-16	Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.
		BT-17	Security tools are deployed and system components are configured to monitor for security-related events.
		BT-18	A static code analysis tool is configured to scan the source code for vulnerabilities.
		BT-48	Customer data is automatically backed up according to a backup configuration scheduled described in the Backup Policy.
		BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.
		BT-58	Applications and system logs are pushed to a central logging repository where possible. Access control to the central repository is enforced based on the Access Control policy. Logs are retained in compliance with applicable legal, regulatory, customer, and operational requirements.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	BT-59	Incidents are recorded and tracked, and all applicable evidence and documentation is reviewed in post-mortem meetings.
		BT-60	The Security Incident Management Program outlines the requirements and process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	BT-59	Incidents are recorded and tracked, and all applicable evidence and documentation is reviewed in post-mortem meetings.
		BT-60	The Security Incident Management Program outlines the requirements and process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	BT-57	OS patches and docker image updates are applied at least weekly.
		BT-59	Incidents are recorded and tracked, and all applicable evidence and documentation is reviewed in post-mortem meetings.
		BT-60	The Security Incident Management Program outlines the requirements and process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.
Change Management			
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	BT-61	The ability to deploy application changes to production environments is restricted to authorized personnel.
		BT-62	The Change Management documentation outlines the internal workflow for propagating application and infrastructure code changes to the production environment, including tracking, testing, reviewing and approving.
		BT-63	All infrastructure is managed as code and follows the standard code review process including approvals and automated testing.
		BT-64	The company uses a version control system to manage source code and documentation, and to implement and run change management functions. The version control software is only accessible by authorized personnel.
		BT-65	The company's software development process includes frequent team meetings which facilitate the communication and evaluation of objectives between team members. These touch points include Scrum meetings, sprint planning, and sprint retrospective meetings.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
		BT-57	OS patches and docker image updates are applied at least weekly.
		BT-66	Change Management procedures are expressed, as much as possible, in appropriate configuration of Continuous Integrations / Continuous Deployment tools, in order to minimize human error and increase auditability of the changes.
		BT-67	All application and infrastructure changes are reviewed by a separate technical resource and approved by authorized personnel before being delivered to the production environment.
		BT-48	Customer data is automatically backed up according to a backup configuration scheduled described in the Backup Policy.
		BT-68	The company maintains separate production and non-production environments.
Risk Mitigation			
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	BT-69	A disaster recovery test with predefined RTO goals is performed annually, assuming a full outage of our primary cloud region.
		BT-70	The company maintains a Business Continuity Policy and Plan which outlines the requirements and a process to recover from prolonged disruptions of business operations.
		BT-29	The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.
		BT-27	The company maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	BT-71	The company maintains an inventory of its vendors and classification of the data they store or process.
		BT-31	Vendors are evaluated on a periodic basis, by reviewing their audit reports or other means, in order to track and determine the impact of any changes in their security posture.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by Interface
		BT-72	As part of the risk management process, vendors storing data classified as Customer Sensitive undergo due diligence and risk assessment.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR: TEST OF CONTROLS

4 INFORMATION PROVIDED BY INDEPENDENT SERVICE AUDITOR EXCEPT FOR APPLICABLE TRUST SERVICES CRITERIA AND CONTROL ACTIVITIES

4.1 Objective of Our Examination

This report, including the description of tests of controls and results thereof in this section are intended solely for the information and use of Interface, user entities of the Interface system related to Interface platform during some or all of the period October 1, 2024 through December 31, 2024, business partners of Interface subject to risks arising from interactions with Interface's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service Organization;
- how the service Organization's system interacts with user entities, subservice Organizations, and other parties;
- internal control and its limitations;
- complementary user-entity controls and how they interact with related controls at the service Organization to meet the applicable trust services criteria; the applicable trust services criteria;
- and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This section presents the following information provided by Interface:

- The controls established and specified by Interface to achieve the specified trust services criteria.

Also included in this section is the following information provided by auditors:

- A description of the tests performed by auditors to determine whether Interface's controls were operating with sufficient effectiveness to achieve specified trust services criteria. Auditors determined the nature, timing, and extent of the testing performed.
- The results of tests of controls.

The examination was conducted in accordance with the criteria as set forth in 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 October 1, 2024 to December 31, 2024 to provide reasonable assurance that Interface's service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, of the American Institute of Certified Public Accountants (AICPA), and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18). SSAE 18 is inclusive of the following: (1) AT-C 105, Concepts Common to all Attestation Engagements; and (2) AT-C 205, Examination Engagements. Our testing of Interface's controls was restricted to the controls identified by Interface to meet the criteria related to Security listed in Section 1 of this report and was not extended to controls described in Section 3 but not included in Section 4, or to controls that may be in effect at user Organizations or subservice Organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and subservice Organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, subservice Organizations, and Interface's controls should be evaluated together. If effective user entity or subservice Organizations controls are not in place, Interface's controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Interface our procedures included tests of the following relevant elements of the Interface control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication
4. Monitoring
5. Control Activities

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Interface activities and operations, inspection of Interface documents and records, and re-performance of the application of Interface controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine the Interface description of the system related to Interface as well as the suitability of the design and operating effectiveness of controls for a representative number of samples throughout the period of October 1, 2024 to December 31, 2024.

In selecting particular tests of the operational effectiveness of controls, we considered the (a) nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the trust services principles and criteria to be achieved and (d) the expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of information provided by Interface is also a component of the testing procedures performed. Information we are utilizing as evidence may include, but is not limited to:

1. Standard 'out of the box' reports as configured within the system
2. Parameter-driven reports generated by Interface systems
3. Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
4. Spreadsheets that include relevant information utilized for the performance or testing of a control
5. Interface - prepared analyses, schedules, or other evidence manually prepared and utilized by the Company

While these procedures are not specifically called out in the test procedures listed in this section, they are completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Interface.

4.4 Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Interface. Our tests of controls were performed on controls as they existed during the period of October 1, 2024 through December 31, 2024, and were applied to those controls relating to the trust services principles and criteria.

Tests performed of the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because auditors does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, auditor reports all deviations.

[Space left blank intentionally]

4.5 Testing Procedures Performed by Independent Service Auditor

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 1.1 CC 1.5 CC 5.3	BT-01	Material violations of the company's Acceptable Use Policy, Code of Conduct, and Information Security policies and procedures applicable to each employee subjects the individual to disciplinary action that could include termination.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Material violations of the company's Acceptable Use Policy, Code of Conduct, and Information Security policies and procedures applicable to each employee subjects the individual to disciplinary action that could include termination.	No exception noted
CC 1.1	BT-02	Organizational values and behavioral standards are communicated to all personnel through an Employee Handbook, which outlines the company's policy regarding Standards of Conduct and Code of Business Ethics.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Organizational values and behavioral standards are communicated to all personnel through an Employee Handbook, which outlines the company's policy regarding Standards of Conduct and Code of Business Ethics.	No exception noted
CC 1.1	BT-03	Company employees are required to sign and attest their adherence to applicable company policies and procedures.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Company employees are required to sign and attest their adherence to applicable company policies and procedures.	No exception noted
CC 1.1	BT-04	All employees and contractors must sign a confidentiality	Enquired with the management regarding the control activity to ascertain that the control	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
		agreement with the company prior to gaining access to any sensitive information.	operates as described. Inspected relevant artefacts to ascertain whether All employees and contractors must sign a confidentiality agreement with the company prior to gaining access to any sensitive information.	
CC 1.1 CC 1.4	BT-05	Background checks are performed on newly hired employees where permitted by law.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Background checks are performed on newly hired employees where permitted by law.	No exception noted
CC 1.1 CC 6.8	BT-06	The Acceptable Use Policy outlines the acceptable use of computer equipment and systems at the company.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether The Acceptable Use Policy outlines the acceptable use of computer equipment and systems at the company.	No exception noted
CC 1.2 CC 1.5 CC 4.1 CC 4.2	BT-07	The company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.	No exception noted
CC 1.2	BT-08	A Board of Directors exercises independent oversight of the company's strategic direction,	Enquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
		operational performance, and internal control.	Inspected relevant artefacts to ascertain whether A Board of Directors exercises independent oversight of the company's strategic direction, operational performance, and internal control.	
CC 1.3	BT-09	The company has an appropriate organizational structure based on functional departments, with an executive leader heading each department.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company has an appropriate organizational structure based on functional departments, with an executive leader heading each department.	No exception noted
CC 1.3	BT-10	Management and the Board of Directors consider requirements relevant to security, availability, processing integrity, and confidentiality. These considerations are documented in the company's Information Security Policy, which specifically delegates the overall responsibility of security to the Security Officer.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Management and the Board of Directors consider requirements relevant to security, availability, processing integrity, and confidentiality. These considerations are documented in the company's Information Security Policy, which specifically delegates the overall responsibility of security to the Security Officer.	No exception noted
CC 1.3 CC 1.4 CC 1.5 CC 2.2	BT-11	Roles and responsibilities of company employees are communicated through documented job descriptions.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Roles and responsibilities of company employees are communicated through documented job descriptions.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 1.4 CC 1.5	BT-12	The company has established a formal review process that includes semi-annual employee self-reviews and immediate manager reviews. Reviews include performance assessments, goal setting, and an evaluation of resources required for the next review period.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company has established a formal review process that includes semi-annual employee self-reviews and immediate manager reviews. Reviews include performance assessments, goal setting, and an evaluation of resources required for the next review period.	No exception noted
CC 1.4 CC 2.2	BT-13	Security awareness training is provided to new employees, and to all employees on a recurring annual basis, to promote strong security practices for the whole company.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Security awareness training is provided to new employees, and to all employees on a recurring annual basis, to promote strong security practices for the whole company.	No exception noted
CC 2.1 CC 3.2 CC 4.1 CC 6.6 CC 7.1 CC 7.2	BT-14	Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.	No exception noted
CC 2.1 CC 2.2 CC 5.1 CC 5.3	BT-15	The company develops and maintains formal policies that govern information security within the company. The policies are	Enquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
		formally reviewed and approved at least once a year, and are communicated to all employees.	Inspected relevant artefacts to ascertain whether the company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.	
CC 2.1 CC 4.1 CC 7.2	BT-16	Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.	No exception noted
CC 2.1 CC 4.1 CC 7.2	BT-17	Security tools are deployed and system components are configured to monitor for security-related events.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Security tools are deployed and system components are configured to monitor for security-related events.	No exception noted
CC 2.1 CC 4.1 CC 7.1 CC 7.2	BT-18	A static code analysis tool is configured to scan the source code for vulnerabilities.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether A static code analysis tool is configured to scan the source code for vulnerabilities.	No exception noted
CC 2.1 CC 3.2 CC 4.1 CC 6.6	BT-19	Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications,	Enquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 7.1 CC 7.2		and issues found are resolved promptly based on severity.	Inspected relevant artefacts to ascertain whether Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.	
CC 2.1 CC 5.3	BT-20	All company and customer data is classified as per the data classification policy.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether All company and customer data is classified as per the data classification policy.	No exception noted
CC 2.2	BT-21	Employees have access to an internal support channel that can be used to report incidents, concerns, and complaints.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Employees have access to an internal support channel that can be used to report incidents, concerns, and complaints.	No exception noted
CC 2.3	BT-22	The company's Privacy Policy is available online to visitors and customers, and outlines the receipt, sharing, use, and disposal of visitor and subscriber data.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company's Privacy Policy is available online to visitors and customers, and outlines the receipt, sharing, use, and disposal of visitor and subscriber data.	No exception noted
CC 2.3	BT-23	The company communicates system changes to its users and customers through an established channel and procedure.	Enquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			Inspected relevant artefacts to ascertain whether the company communicates system changes to its users and customers through an established channel and procedure.	
CC 2.3	BT-24	The company maintains a customer-accessible technical documentation site containing high-level overviews and detailed information about the company's products and services, including security-oriented articles and guides.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains a customer-accessible technical documentation site containing high-level overviews and detailed information about the company's products and services, including security-oriented articles and guides.	No exception noted
CC 2.3	BT-25	External users are provided with a support channel for reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether External users are provided with a support channel for reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.	No exception noted
CC 2.3	BT-26	The company's Terms of Use are available online to visitors and customers, and outline the requirements and commitments of both parties relative to security and confidentiality.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company's Terms of Use are available online to visitors and customers, and outline the requirements and commitments of both parties relative to security and confidentiality.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 3.1 CC 9.1	BT-27	The company maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.	No exception noted
CC 3.2 CC 6.1	BT-28	The company maintains an inventory of IT infrastructure devices.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains an inventory of IT infrastructure devices.	No exception noted
CC 3.2 CC 3.4 CC 5.1 CC 5.2 CC 9.1	BT-29	The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.	No exception noted
CC 3.3	BT-30	The company assesses the potential for fraud from internal or external stakeholders as part of its Risk Assessment process.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company assesses the potential for fraud from internal or external stakeholders as part of its Risk Assessment process.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 3.4 CC 9.2	BT-31	Vendors are evaluated on a periodic basis, by reviewing their audit reports or other means, in order to track and determine the impact of any changes in their security posture.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Vendors are evaluated on a periodic basis, by reviewing their audit reports or other means, in order to track and determine the impact of any changes in their security posture.	No exception noted
CC 5.1 CC 5.2	BT-32	The company designs and implements controls to mitigate risks identified during the risk assessment process.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company designs and implements controls to mitigate risks identified during the risk assessment process.	No exception noted
CC 5.1 CC 5.2	BT-33	Management periodically reviews control activities to reaffirm each control's relevance, and updates the set of controls as necessary.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Management periodically reviews control activities to reaffirm each control's relevance, and updates the set of controls as necessary.	No exception noted
CC 5.2	BT-34	Control activities over the technology infrastructure and technology access control are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Control activities over the technology infrastructure and technology access control are designed and implemented to help ensure the	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			completeness, accuracy, and availability of technology processing.	
CC 5.3	BT-35	Control owners take corrective actions when issues and nonconformities with their controls are identified.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Control owners take corrective actions when issues and nonconformities with their controls are identified.	No exception noted
CC 6.1	BT-36	The company leverages SSO authentication for sensitive systems, wherever available.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company leverages SSO authentication for sensitive systems, wherever available.	No exception noted
CC 6.1	BT-37	All users with privileged access to sensitive systems are required to use a password management solution.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether All users with privileged access to sensitive systems are required to use a password management solution.	No exception noted
CC 6.1 CC 6.2	BT-38	Access to sensitive systems and resources is granted based on the principle of least privilege.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Access to sensitive systems and resources is granted based on the principle of least privilege.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 6.1	BT-39	The company maintains an inventory of all information systems, services, and assets, and classifies them based on the data they store. Inventory is reviewed as part of an annual Risk Assessment.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains an inventory of all information systems, services, and assets, and classifies them based on the data they store. Inventory is reviewed as part of an annual Risk Assessment.	No exception noted
CC 6.1 CC 6.3	BT-40	Defined permission roles are utilized to assign and segregate access privileges to data and systems.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Defined permission roles are utilized to assign and segregate access privileges to data and systems.	No exception noted
CC 6.1 CC 6.3	BT-41	Administrative access privileges for sensitive systems are only granted to a restricted, small set of personnel, with a clearly defined business need to maintain and administer those systems.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether administrative access privileges for sensitive systems are only granted to a restricted, small set of personnel, with a clearly defined business need to maintain and administer those systems.	No exception noted
CC 6.1	BT-42	Access to sensitive systems requires multi-factor authentication.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Access to sensitive systems requires multi-factor authentication.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 6.1 CC 6.2 CC 6.3	BT-43	Password configuration settings are managed in compliance with the company's Password Policy.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Password configuration settings are managed in compliance with the company's Password Policy.	No exception noted
CC 6.1 CC 6.6 CC 6.7	BT-44	The company maintains documented guidance on the selection and configuration of appropriate cryptographic methods.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains documented guidance on the selection and configuration of appropriate cryptographic methods.	No exception noted
CC 6.2 CC 6.3	BT-45	Termination checklists are executed upon separation with an employee or contractor to ensure asset return, and prompt and complete access revocation.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Termination checklists are executed upon separation with an employee or contractor to ensure asset return, and prompt and complete access revocation.	No exception noted
CC 6.2 CC 6.3	BT-46	Access to systems is requested by filing an internal access request ticket specifying the need for the access. Access is approved by the respective manager and granted by administrators based on a least-privilege principle.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Access to systems is requested by filing an internal access request ticket specifying the need for the access. Access is approved by the	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			respective manager and granted by administrators based on a least-privilege principle.	
CC 6.2 CC 6.3	BT-47	A review of users with access to Customer Confidential systems is performed periodically to ensure that access is restricted to appropriate personnel.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether A review of users with access to Customer Confidential systems is performed periodically to ensure that access is restricted to appropriate personnel.	No exception noted
CC 6.5	BT-49	Customer data is securely disposed of after its retention period passes, and any retained data is sanitized and anonymized.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Customer data is securely disposed of after its retention period passes, and any retained data is sanitized and anonymized.	No exception noted
CC 6.5	BT-50	Retention periods for customer data are specified in the company's Data Retention Procedure and adhere to compliance, regulatory, contractual, and organizational requirements.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Retention periods for customer data are specified in the company's Data Retention Procedure and adhere to compliance, regulatory, contractual, and organizational requirements.	No exception noted
CC 6.6 CC 6.7	BT-51	Firewalls are configured to restrict network traffic to the minimum required for the system to function.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			Firewalls are configured to restrict network traffic to the minimum required for the system to function.	
CC 6.6 CC 6.7	BT-52	TLS usage is evaluated on a quarterly basis using tools such as ssllabs and any grades lower than A are promptly corrected.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether TLS usage is evaluated on a quarterly basis using tools such as ssllabs and any grades lower than A are promptly corrected.	No exception noted
CC 6.7	BT-53	Data stores are configured to enable encryption at rest.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Data stores are configured to enable encryption at rest.	No exception noted
CC 6.7	BT-54	Data in transit over the public Internet is encrypted with industry-standard algorithms.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Data in transit over the public Internet is encrypted with industry-standard algorithms.	No exception noted
CC 6.7	BT-55	Third-party cloud filestores such as S3 and GCS are configured with a minimum server-side encryption using the vendor's key.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Third-party cloud filestores such as S3 and GCS are configured with a minimum server-side encryption using the vendor's key.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
CC 6.8	BT-56	The company monitors the IT infrastructure devices for compliance with the Asset Management Policy and checks for requirements such as hard drive encryption, user authentication requirements, and security patching.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company monitors the IT infrastructure devices for compliance with the Asset Management Policy and checks for requirements such as hard drive encryption, user authentication requirements, and security patching.	No exception noted
CC 6.8 CC 7.5 CC 8.1	BT-57	OS patches and docker image updates are applied at least weekly.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether OS patches and docker image updates are applied at least weekly.	No exception noted
CC 7.2 CC 8.1	BT-48	Customer data is automatically backed up according to a backup configuration scheduled described in the Backup Policy.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Customer data is automatically backed up according to a backup configuration scheduled described in the Backup Policy.	No exception noted
CC 7.2	BT-58	Applications and system logs are pushed to a central logging repository where possible. Access control to the central repository is enforced based on the Access Control policy. Logs are retained in compliance with applicable legal, regulatory, customer, and operational requirements.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Applications and system logs are pushed to a central logging repository where possible. Access control to the central repository is enforced based on the Access Control policy. Logs are retained in	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			compliance with applicable legal, regulatory, customer, and operational requirements.	
CC 7.3 CC 7.4 CC 7.5	BT-59	Incidents are recorded and tracked, and all applicable evidence and documentation is reviewed in post-mortem meetings.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Incidents are recorded and tracked, and all applicable evidence and documentation is reviewed in post-mortem meetings.	No exception noted
CC 7.3 CC 7.4 CC 7.5	BT-60	The Security Incident Management Program outlines the requirements and process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether The Security Incident Management Program outlines the requirements and process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.	No exception noted
CC 8.1	BT-61	The ability to deploy application changes to production environments is restricted to authorized personnel.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the ability to deploy application changes to production environments is restricted to authorized personnel.	No exception noted
CC 8.1	BT-62	The Change Management documentation outlines the internal workflow for propagating application and infrastructure	Enquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
		code changes to the production environment, including tracking, testing, reviewing and approving.	Inspected relevant artefacts to ascertain whether The Change Management documentation outlines the internal workflow for propagating application and infrastructure code changes to the production environment, including tracking, testing, reviewing and approving.	
CC 8.1	BT-63	All infrastructure is managed as code and follows the standard code review process including approvals and automated testing.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether All infrastructure is managed as code and follows the standard code review process including approvals and automated testing.	No exception noted
CC 8.1	BT-64	The company uses a version control system to manage source code and documentation, and to implement and run change management functions. The version control software is only accessible by authorized personnel.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company uses a version control system to manage source code and documentation, and to implement and run change management functions. The version control software is only accessible by authorized personnel.	No exception noted
CC 8.1	BT-65	The company's software development process includes frequent team meetings which facilitate the communication and evaluation of objectives between team members. These touch points include Scrum meetings, sprint planning, and sprint retrospective meetings.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company's software development process includes frequent team meetings which facilitate the communication and evaluation of objectives between team members. These touch points	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			include Scrum meetings, sprint planning, and sprint retrospective meetings.	
CC 8.1	BT-66	Change Management procedures are expressed, as much as possible, in appropriate configuration of Continuous Integrations / Continuous Deployment tools, in order to minimize human error and increase auditability of the changes.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether Change Management procedures are expressed, as much as possible, in appropriate configuration of Continuous Integrations / Continuous Deployment tools, in order to minimize human error and increase auditability of the changes.	No exception noted
CC 8.1	BT-67	All application and infrastructure changes are reviewed by a separate technical resource and approved by authorized personnel before being delivered to the production environment.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether All application and infrastructure changes are reviewed by a separate technical resource and approved by authorized personnel before being delivered to the production environment.	No exception noted
CC 8.1	BT-68	The company maintains separate production and non-production environments.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains separate production and non-production environments.	No exception noted
CC 9.1	BT-69	A disaster recovery test with predefined RTO goals is performed annually, assuming a full outage of our primary cloud region.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether	No exception noted

TSC Ref. #	Control Ref. #	Control Activities as specified by Interface	Testing Performed	Results of Tests
			A disaster recovery test with predefined RTO goals is performed annually, assuming a full outage of our primary cloud region.	
CC 9.1	BT-70	The company maintains a Business Continuity Policy and Plan which outlines the requirements and a process to recover from prolonged disruptions of business operations.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains a Business Continuity Policy and Plan which outlines the requirements and a process to recover from prolonged disruptions of business operations.	No exception noted
CC 9.2	BT-71	The company maintains an inventory of its vendors and classification of the data they store or process.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether the company maintains an inventory of its vendors and classification of the data they store or process.	No exception noted
CC 9.2	BT-72	As part of the risk management process, vendors storing data classified as Customer Sensitive undergo due diligence and risk assessment.	Enquired with the management regarding the control activity to ascertain that the control operates as described. Inspected relevant artefacts to ascertain whether as part of the risk management process, vendors storing data classified as Customer Sensitive undergo due diligence and risk assessment.	No exception noted