FRAGMENT

# Form 046

# SOC 2, TYPE II

# Audit Report

## for the period of February 15, 2026 – May 15, 2026

CONTROLS IN OPERATION AT FRAGMENT COVERING SECURITY TRUST SERVICES CRITERIA

June 4, 2026

| Author | Role | Date | Comments |
|---|---|---|---|
| Fakhar Salahuddin | Audit Team Member | 12-MAY-2026 | Initial Draft |
| Joseph Weindorfer, CPA | CPA Review | 01-JUN-2026 | Technical Review |
| Thomas Craft | Quality Review | 04-JUN-2026 | QA/Visual Review |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

# Table of Contents

# Type II System and Organization Controls Report (SOC 2)

This report details the Fragment service organization's Description of its system and the suitability of the design and operating effectiveness of its controls relevant to Security for the period of February 15, 2026 – May 15, 2026.

**Report Sections**

1. Assertion of Fragment Management
2. Independent Service Auditor's Report
3. Description of Fragment service Organization System
4. Trust Service Categories, Criteria, Related Controls, and Tests of Controls



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

# 1 SECTION I: Assertion of Fragment Management

We have prepared the accompanying description in Section 3, titled ”Fragment Service Organization’s Description of Its Infrastructure Services System (the “system”) for the Period of February 15, 2026 – May 15, 2026,” based on the criteria for a description of a service organization’s system in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2®Report (AICPA, *Description Criteria)* (the “description criteria”).

The description is intended to provide report users with information about the Infrastructure Services System that may be useful when assessing the risks arising from interactions with Fragment service organization’s system, particularly information about system controls that Fragment 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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Fragment service organization uses a subservice organization for cloud hosting services.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fragment service organization, to achieve Fragment service organization’s service commitments and system requirements based on the applicable trust services criteria.

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

a) The description presents Fragment service organization’s Infrastructure Services System that was designed and implemented for the period of February 15, 2026 – May 15, 2026, in accordance with the aforementioned description criteria.

b) The controls stated in the description were suitably designed for the period of February 15, 2026 – May 15, 2026, to provide reasonable assurance that Fragment service organization’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period.

c) The controls stated in the description operated effectively for the period of February 15, 2026 – May 15, 2026, to provide reasonable assurance that Fragment service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Fragment controls operated effectively throughout that period.



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

# 2 SECTION II: Independent Service Auditor's Report

## 2.1 Scope

We have examined Fragment's accompanying description in Section 3, titled "Fragment Service Organization's Description of Its Infrastructure Services System (the "description") for the Period of February 15, 2026 – May 15, 2026," based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)* (the "description criteria") and the suitability of the design and operating effectiveness of controls stated in the description For the period of February 15, 2026-May 15, 2026, to provide reasonable assurance that Fragment's service commitments and system requirements were achieved based on the trust services criteria relevant to *Security* (the "applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

## 2.2 Service Organization's Responsibilities

Fragment service organization is responsible for providing the services covered by the description; specifying its service commitments and system requirements; identifying the risks that threaten the achievement of the service organization's service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Fragment service commitments and system requirements and its business objectives, *Security* requirements and compliance obligations were achieved; preparing the description, including stating the related controls in the description and the completeness, accuracy, and method of presentation of the description; and selecting the applicable trust services criteria as the criteria against which the controls were measured. Fragment service organization has provided the accompanying assertion, in Section 1, ("assertion") about the description, the suitability of design, and the operating effectiveness of controls. Fragment is also responsible for the completeness, accuracy, and method of presentation of the assertion.

## 2.3 Service Auditor's Responsibilities

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

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

- *Obtaining an understanding of the system and the service organization's service commitments and system requirements*
- *Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively*
- *Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria*
- *Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria*
- *Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria*
- *Evaluating the overall presentation of the description.*

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

The examination was conducted under the responsibility of an individual licensed Certified Public Accountant.

## 2.4 Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or 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 policies or procedures may deteriorate.

## 2.5 Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests, are presented in the test matrices in Section 4 of our report titled "Applicable Trust Service Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests."

## 2.6 Opinion

In our opinion, in all material respects,

a) The description presents Fragment service organization's infrastructure services system that was designed and implemented for the period of February 15, 2026 – May 15, 2026, in accordance with the description criteria; and,

b) The controls stated in the description were suitably designed for the period of February 15, 2026 – May 15, 2026, to provide reasonable assurance that Fragment service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria and its business objectives, *Security* requirements, and compliance obligations would be achieved based on applicable trust services criteria throughout that period.

c) The controls stated in the description operated effectively for the period of February 15, 2026 – May 15, 2026, to provide reasonable assurance that Fragment service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Fragment controls operated effectively throughout that period.

## 2.7 Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Fragment service organization; user entities of Fragment service organization's Infrastructure Services system for the period of February 15, 2026 – May 15, 2026; business partners of Fragment service organization subject to risks arising from interactions with the infrastructure services system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; regulators; and sponsoring organizations who have sufficient knowledge and understanding of the following:

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

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

**Signature:** Joseph Weindorfer **Date:** 2026-06-24

**Joseph Weindorfer, CPA**

**CISSP, ITiL, MCSE, M.S**

# 3 SECTION III: Fragment Service Organization's Description of Its Infrastructure Services System for the Period of February 15, 2026 – May 15, 2026

## 3.1 Company Background

Fragment Foundries Inc is a financial technology company building a ledger API and developer tools to support companies building products that move money. We are fully remote with employees in New York, San Francisco, Vancouver, and Sydney Australia.

## 3.2 Description of Services Overview

The Fragment Platform provides customers with a Ledger API, language specific SDKs, and user-facing Dashboard to build and manage their Ledger data.

The Fragment Platform facilitates: user onboarding, API client management, permissioning, ledger schema design, and data retrieval. In addition, Fragment works closely with customers to help translate their product funds flows into the Fragment Platform during their onboarding process.

## 3.3 Principal Service Commitments and System Requirements

Fragment Foundries Inc designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Fragment Foundries Inc makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Fragment Foundries Inc has established for the services. The system services are subject to the Security commitments established internally for its services.

Fragments' commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, and in the description of the service offering provided online at fragment.dev

## 3.4 Security Commitments

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures

- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

## 3.5 Components of the System

The System description is comprised of the following components:

- **Software –** The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- **People –** The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- **Data –** The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- **Procedures –** The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

## 3.6 Infrastructure

Fragment Foundries Inc maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

| Hardware | Type | Purpose (optional) |
|---|---|---|
| AWS Elastic Compute Cloud (EC2) | AWS | |
| AWS Elastic Load Balancers | AWS | Load balance internal and external traffic |
| Virtual Private Cloud | AWS | Protects the network perimeter and restricts inbound and outbound access |
| S3 Buckets | AWS | Storage, upload and download |

## 3.7 Software

Fragment Foundries Inc is responsible for managing the development and operation of the Fragment Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Fragment Foundries Inc infrastructure and software components are shown in the table provided below:

| System / Application | Operating System | Purpose |
|---|---|---|
| GuardDuty | AWS | Security application used for automated intrusion detection (IDS) |
| Datadog | Datadog | Monitoring application used to provide monitoring, alter, and notification services for Fragment Foundries Inc platform |
| Amazon Web Services | | |
| Certn (Partner) | | |
| GitHub | | |
| Google Drive | | |
| Google Workspace | | |
| Justworks | | |
| Linear | | |
| Slack | | |
| Vanta | | |

## 3.8 People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Fragment Foundries Inc has a staff of approximately 8 organized in the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

  This includes:

  - CEO - Thomas Neckel
  - Head of Engineering - Varun Mohan

- **Operations:** Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.
- **Information Technology:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Product Development:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

## 3.9 Data

Data as defined by Fragment Foundries Inc, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Fragment Foundries Inc

| Category | Description | Examples |
|---|---|---|
| Public | Public information is not confidential and can be made public without any implications for Fragment Foundries Inc. | • Press releases<br>• Public website |
| Internal | Access to internal information is approved by management and is protected from external access. | • Internal memos<br>• Design documents<br>• Product specifications<br>• Correspondences |

| | | |
|---|---|---|
| Customer data | Information received from customers for processing or storage by Fragment Foundries Inc. Fragment Foundries Inc must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information. | • Customer operating data<br>• Customer PII<br>• Customers' customers' PII<br>• Anything subject to a confidentiality agreement with a customer |
| Company data | Information collected and used by Fragment Foundries Inc to operate the business. Fragment Foundries Inc must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information. | • Legal documents<br>• Contractual agreements<br>• Employee PII<br>• Employee salaries |

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Fragment Foundries Inc has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

## 3.10Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

## 3.11 Physical Security

Fragment Foundries Inc's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Fragment Foundries Inc reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

## 3.12 Logical Access

Fragment Foundries Inc provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

Operations, Management is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Fragment Foundries Inc's policies, completing security training. These steps must be completed within 7 days of hire.

When an employee is terminated, Operations, Management is responsible for deprovisioning access to all in scope systems within 24 hours for that employee's termination.

## 3.13 Computer Operations - Backups

Customer data is backed up and monitored by the Engineering, Head of Engineering for completion and exceptions. If there is an exception, Engineering, Head of Engineering will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

## 3.14 Computer Operations - Availability

Fragment Foundries Inc maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Fragment Foundries Inc internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Fragment Foundries Inc utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

## 3.15 Change Management

Fragment Foundries Inc maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure

changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

## 3.16 Data Communications

Fragment Foundries Inc has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Fragment Foundries Inc application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Fragment uses an automated monitoring service to perform vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

## 3.17 Boundaries of the System

The boundaries of the Fragment Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Fragment Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

## 3.18 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 Fragment Foundries Inc's control environment, affecting the design, administration, and monitoring of other

components. Integrity and ethical behavior are the product of Fragment Foundries Inc's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

## 3.19Commitment to Competence

Fragment Foundries Inc's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

## 3.20Management's Philosophy and Operating Style

The Fragment Foundries Inc management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Fragment Foundries Inc can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Fragment Foundries Inc to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

## 3.21 Organizational Structure and Assignment of Authority and Responsibility

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

Fragment Foundries Inc's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It 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.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

## 3.22 HR Policies and Practices

Fragment Foundries Inc's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Fragment Foundries Inc's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.

- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

## 3.23 Risk Assessment Process

Fragment Foundries Inc's risk assessment process identifies and manages risks that could potentially affect Fragment Foundries Inc's ability to provide reliable and secure services to our customers. As part of this process, Fragment Foundries Inc maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Fragment Foundries Inc product development process so they can be dealt with predictably and iteratively.

## 3.24 Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Fragment Foundries Inc's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Fragment Foundries Inc addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Fragment Foundries Inc's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

## 3.25 Information and Communication Systems

Information and communication are an integral component of Fragment Foundries Inc's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Fragment Foundries Inc uses several information and communication channels internally to share information with management, employees, contractors, and customers. Fragment Foundries Inc uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Fragment Foundries Inc uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

## 3.26 Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Fragment Foundries Inc's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence

to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

## 3.27Ongoing Monitoring

Fragment Foundries Inc's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Fragment Foundries Inc's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Fragment Foundries Inc's personnel.

## 3.28Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## 3.29Changes to the System

No significant changes have occurred to the services provided to user entities during the review period or since the organization's last review.

## 3.30Incidents

No significant incidents have occurred to the services provided to user entities during the review period or since the organization's last review.

## 3.31Criteria Not Applicable to the System

All Common Criteria/Security, Security criteria were applicable to the Fragment Foundries Inc's Fragment Platform system.

## 3.32Subservice Organizations

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

## 3.33Subservice Description of Services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

## 3.34Complementary Subservice Organization Controls

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

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

| AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Security | CC 6.4 | Physical access to data centers is approved by an authorized individual. |
| Security | CC 6.4 | Physical access is revoked within 24 hours of the employee or vendor record being deactivated. |
| Security | CC 6.4 | Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. |
| Security | CC 6.4 | Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. |
| Security | CC 6.4 | Access to server locations is managed by electronic access control devices. |
| Availability | A 1.2 | AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. |
| Availability | A 1.2 | AWS has a process in place to review environmental and geo-political risks before launching a new region. |
| Availability | A 1.2 | Amazon-owned data centers are protected by fire detection and suppression systems. |

| | | |
|---|---|---|
| Availability | A 1.2 | Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels. |
| Availability | A 1.2 | Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers |
| Availability | A 1.2 | Amazon-owned data centers have generators to provide backup power in case of electrical failure. |
| Availability | A 1.2 | Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS. |

Fragment Foundries Inc management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Fragment Foundries Inc performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

## 3.35Complementary User Entity Controls

Fragment Foundries Inc's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Fragment Foundries Inc's services to be solely achieved by Fragment Foundries Inc control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Fragment Foundries Inc's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items

represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Fragment Foundries Inc.
2. User entities are responsible for notifying Fragment Foundries Inc of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Fragment Foundries Inc services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Fragment Foundries Inc services.
6. User entities are responsible for providing Fragment Foundries Inc with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Fragment Foundries Inc of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

# 4 SECTION IV: Applicable Trust Service Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

## 4.1 Security Trust Criteria

### 4.1.1 Control Environment

| TSC ref. # CC1.1 - The entity demonstrates a commitment to integrity and ethical values. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC1.1.1** The Organization requires contractor agreements to include a code of conduct or reference to the Organization code of conduct. | Reviewed Fragment's Human Resource Security Policy and contractor agreement templates and onboarding documentation reflecting inclusion of code of conduct terms or reference to the organizational Code of Conduct.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that all contractors must accept and comply with the company's Code of Conduct as part of engagement requirements on the Vanta Compliance Platform.<br><br>Reviewed the onboarding process for full time employees and contractors, the HR process is same from employees and contractors, there are no contractors hired during the observation period, although the process for contractor onboarding has been reviewed. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC1.1.2** The Organization requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Reviewed Fragment's Human Resource Security Policy, including Code of Conduct requirements and disciplinary policy documentation. Verified onboarding checklists requiring acknowledgment upon hiring.<br><br>Interviewed the Head of IT and Co-Founder and confirmed employee adherence is monitored and disciplinary actions are enforced when violations occur.<br><br>Observed sample signed Code of Conduct acknowledgment forms stored as part of personnel documentation confirming compliance at time of hire for PM, who joined on 29-Jan-2026. There were no new onboardings during the observation period. | No Exception |
| **TSC ref # CC1.1.3** The Organization requires contractors to sign a confidentiality agreement at the time of engagement. | Reviewed contractor engagement procedures and confidentiality agreement templates included in standard onboarding documentation.<br><br>Interviewed the Head of IT and Co-Founder and confirmed confidentiality agreement execution is mandatory prior to access being granted.<br><br>Observed executed confidentiality agreements maintained for contractors to validate compliance. There were no new contractors hired during the observation period. | No Exception |
| **TSC ref # CC1.1.4** The Organization requires employees to sign a confidentiality agreement during onboarding. | Reviewed onboarding process and confidentiality agreement templates integrated into hiring workflows.<br>- Reviewed and verified records for a new hire PM, who joined in Jan-2026.<br><br>Interviewed the Head of IT and Co-Founder and confirmed procedure enforcement and tracking through the onboarding process.<br><br>Observed signed confidentiality agreements retained within employee personnel records. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC1.1.5** The Organization performs background checks on new employees. | Reviewed hiring policies describing mandatory background checks prior to final employment confirmation, along with sample background verification records.<br>Interviewed the Head of IT and Co-Founder and confirmed that checks are performed to validate employment eligibility and reliability.<br>A third-party vendor – Certn – is used for background verifications.<br>Observed documented background clearance results for PM, who joined in Jan-2026. | No Exception |
| **TSC ref # CC1.1.6** The Organization managers are required to complete performance evaluations for direct reports at least annually. | Inspected the Performance Management Policy and the annual review schedule, which defines responsibilities for managers and Human Resources in conducting employee performance evaluations.<br>Conducted discussions with the Head of IT and Co-Founder regarding the performance evaluation process and management's oversight for tracking completion of annual reviews.<br>Validated through inspection of the performance evaluation template and related documentation that a formal review process has been established. | **Exception Noted:**<br>The organization has not conducted a formal performance evaluation as per the defined policy for the in-scope employees. |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC1.2 - The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC1.2.1** The Organization's board of directors has a documented charter that outlines its oversight responsibilities for internal control. | Reviewed the Monthly and Weekly Executive Meeting records defining responsibilities related to governance, oversight of internal controls, and organizational risk management.<br><br>Fragment's Board comprises the Founder, Co-Founder Tom, and an investor who joined the Board last year. While a formal documented Board Charter was not observed during the review period (15-Feb-2026 – 15-May-2026), the organization demonstrates active Board-level oversight through defined roles and responsibilities within the leadership team. The Board conducts monthly meetings dedicated to operational oversight and business planning, in addition to bi-weekly strategic meetings ensuring ongoing governance across the Organization. The Founder and Co-Founder are actively involved in day-to-day oversight of internal controls and operations. | No Exception |
| **TSC ref # CC1.2.2** The Organization's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed. | Reviewed competency requirements and governance documentation indicating skill criteria for cybersecurity oversight and use of external subject matter experts when appropriate.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that internal security expertise is supplemented through external advisory support for planning and risk-based decision making.<br><br>Reviewed the resumes of Board members (i.e., TN, OC, and VM).<br><br>Observed evidence of Executive Leadership meeting s conducted on monthly basis.<br>- Reviewed the meeting minutes for JAN, FEB, and APR 2026. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC1.2.3** The Organization's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the Organization. | Reviewed Board Charter and Governance policies describing Board meeting frequency, independence criteria, and documentation requirements. Examined Board meeting minutes demonstrating adherence to quarterly oversight obligations.<br>Interviewed the Head of IT and Co-Founder and confirmed meetings are held at defined intervals and formally documented.<br>Observed records of Executive Meeting minutes, including attendance details, for JAN, FEB, and APR 2026. | No Exception |
| **TSC ref # CC1.2.4** The Organization's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the Organization's cybersecurity and privacy risk. The board provides feedback and direction to management as needed. | Reviewed the Monthly Executive Meeting minutes defining responsibilities related to governance, oversight of internal controls, and organizational risk management.<br>Fragment’s leadership team actively promotes ethical values through key practices like transparent communication and Equal Treatment Policy.<br>Interviewed the Head of IT and Co-Founder and confirmed that the Board charter is reviewed periodically to ensure responsibilities remain aligned with organizational needs and regulatory expectations.<br>Observed current governance documentation including charter approval records demonstrating the Board’s oversight role. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC 1.3.1** The Organization management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Reviewed Fragment's Information Security Roles and Responsibilities policy document including security responsibility matrices and policy assignments that define accountability for security control design and implementation.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that leadership teams actively manage information security responsibilities and ensure alignment with operational and business objectives.<br><br>Observed documented position accountability and oversight responsibilities supporting effective governance of information security controls such as Senior Management, Engineering Leadership, Security officer, Application Owners, and Staff. | No Exception |
| **TSC ref # CC1.3.2** The Organization maintains an organizational chart that describes the organizational structure and reporting lines. | Reviewed the approved organizational structure that outlines reporting hierarchy and key functional roles within the company.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that organizational charts are updated as needed and distributed internally for clarity on authority and communication flow.<br><br>Observed current organizational chart updated May-2026, with documentation depicting reporting lines, supporting accountability, and structured oversight. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC1.3.3** Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Reviewed the information security job roles and responsibilities documents along with the organizational chart defining responsibilities for managing information security controls throughout the technology environment lifecycle.<br>Interviewed the Head of IT and Co-Founder and confirmed staff responsibilities are assigned and communicated during onboarding and role transitions.<br>Reviewed the job descriptions for Head of IT, Head of Engineering, Engineering Team, and Designers<br>Observed evidence of documented job responsibilities and acknowledgment supporting accountability for security-related duties. | No Exception |
| **TSC ref# CC1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC1.4.1** The Organization performs background checks on new employees. | Reviewed hiring policies describing mandatory background checks prior to final employment confirmation, along with sample background verification records.<br>Interviewed the Head of IT and Co-Founder and confirmed that checks are performed to validate employment eligibility and reliability.<br>A third-party vendor – Certn – is used for background verifications.<br>Observed documented background clearance results for PM, who joined in Jan-2026. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC1.4.2** The Organization managers are required to complete performance evaluations for direct reports at least annually. | Inspected the Performance Management Policy and the annual review schedule, which defines responsibilities for managers and Human Resources in conducting employee performance evaluations.<br><br>Conducted discussions with the Head of IT and Co-Founder regarding the performance evaluation process and management's oversight for tracking completion of annual reviews.<br><br>Validated through inspection of the performance evaluation template and related documentation that a formal review process has been established. | **Exception Noted:**<br><br>See **TSC ref # CC1.1.6** |
| **TSC ref # CC1.4.3** Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Reviewed the information security job roles and responsibilities documents along with the organizational chart defining responsibilities for managing information security controls throughout the technology environment lifecycle.<br><br>Interviewed the Head of IT and Co-Founder and confirmed staff responsibilities are assigned and communicated during onboarding and role transitions.<br><br>Reviewed the job descriptions for Head of IT, Head of Engineering, Engineering Team, and Designers<br><br>Observed evidence of documented job responsibilities and acknowledgment supporting accountability for security-related duties. | No Exception |
| **TSC ref # CC1.4.4** The Organization requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Reviewed Fragment's Human Resource Policy documentation requiring onboarding and recurring cybersecurity awareness training.<br><br>Interviewed the Head of IT and Co-Founder and confirmed training completion is tracked, and follow-ups are made for overdue staff on the compliance platform.<br><br>Observed security awareness training completion records demonstrating adherence to annual awareness training requirements on the Vanta compliance platform for all contractors and new hires during the observation period. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC1.5.1** The Organization requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Reviewed Fragment's Human Resource Security Policy, including Code of Conduct requirements and disciplinary policy documentation. Verified onboarding checklists requiring acknowledgment upon hiring.<br><br>Interviewed the Head of IT and Co-Founder and confirmed employee adherence is monitored and disciplinary actions are enforced when violations occur.<br><br>Observed sample signed Code of Conduct acknowledgment forms stored as part of personnel documentation confirming compliance at time of hire for PM, who joined on 29-Jan-2026. There were no new onboardings during the observation period. | No Exception |
| **TSC ref # CC1.5.2** The Organization managers are required to complete performance evaluations for direct reports at least annually. | Inspected the Performance Management Policy and the annual review schedule, which defines responsibilities for managers and Human Resources in conducting employee performance evaluations.<br><br>Conducted discussions with the Head of IT and Co-Founder regarding the performance evaluation process and management's oversight for tracking completion of annual reviews.<br><br>Validated through inspection of the performance evaluation template and related documentation that a formal review process has been established. | **Exception Noted:**<br><br>See<br>**TSC ref # CC1.1.6** |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC1.5.3** Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Reviewed the information security job roles and responsibilities documents along with the organizational chart defining responsibilities for managing information security controls throughout the technology environment lifecycle.<br><br>Interviewed the Head of IT and Co-Founder and confirmed staff responsibilities are assigned and communicated during onboarding and role transitions.<br><br>Reviewed the job descriptions for Head of IT, Head of Engineering, Engineering Team, and Designers.<br><br>Observed evidence of documented job responsibilities and acknowledgment supporting accountability for security-related duties. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.2 Communication and Information

| TCS ref # CC 2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC2.1.1** The Organization performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the Organization has committed to an SLA for a finding, the corrective action is completed within that SLA. | Reviewed Fragment's Operational Security Policy and annual internal control self-assessment documentation, corrective action tracking logs, and remediation tracking procedures outlining timelines and SLA compliance.<br>Interviewed the Head of IT and Co-Founder and confirmed that senior leadership oversees control assessments and remediation progress through structured review meetings on a weekly basis.<br>Observed completed control assessment reports and evidence of open and closed remediation tasks tracked to completion within agreed timelines.<br>Reviewed the external penetration test reports and remediation actions.<br>The organization also relies on Vanta compliance platform for security posture assessment through implemented controls. | No Exception |
| **TSC ref # CC2.1.2** The Organization utilizes a log management tool to identify events that may have a potential impact on the Organization's ability to achieve its security objectives. | Reviewed log management configuration documentation and event monitoring procedures outlining how system activity is monitored and analyzed for security-related events.<br>Interviewed the Head of IT and Co-Founder and confirmed that logs are reviewed regularly and alerts are escalated per defined thresholds.<br>AWS Native Applications are implemented to observe any abnormal behaviors of the cloud infrastructure. Alerts are instantly reviewed by the DevOps teams.<br>AWS GuardDuty and CloudWatch are integrated for security and observability alerts.<br>Observed screenshots/log samples demonstrating active event logging and timely alert generation for abnormal or unauthorized activities. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC2.1.3** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC 2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC2.2.1** The Organization has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Reviewed incident response policies, incident reporting workflows, and communication protocols that define how personnel must report and respond to cybersecurity and privacy incidents.<br>Interviewed the Head of IT and Co-Founder and confirmed that employees are informed of reporting channels and escalation expectations during onboarding and refresher training.<br>Observed access to incident response documentation on internal platforms (i.e., Slack).<br>Reviewed the one incident related to the service downtime.<br>The organization uses the incident management platform Incident.io for incident tracking. | No Exception |
| **TSC ref # CC2.2.2** The Organization management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Reviewed Fragment's Information Security Roles and Responsibilities policy document, including security responsibility matrices and policy assignments that define accountability for security control design and implementation.<br>Interviewed the Head of IT and Co-Founder and confirmed that leadership teams actively manage information security responsibilities and ensure alignment with operational and business objectives.<br>Observed documented position accountability and oversight responsibilities supporting effective governance of information security controls such as Senior Management, Engineering Leadership, Security officer, Application Owners, and Staff. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC2.2.3** Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Reviewed the information security job roles and responsibilities documents along with the organizational chart defining responsibilities for managing information security controls throughout the technology environment lifecycle.<br>Interviewed the Head of IT and Co-Founder and confirmed staff responsibilities are assigned and communicated during onboarding and role transitions.<br>Reviewed the Job descriptions for Head of IT, Head of Engineering, Engineering Team, and Designers.<br>Observed evidence of documented job responsibilities and acknowledgment supporting accountability for security-related duties. | No Exception |
| **TSC ref # CC2.2.4** The Organization requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Reviewed Fragment's Human Resource Policy documentation requiring onboarding and recurring cybersecurity awareness training.<br>Interviewed the Head of IT and Co-Founder and confirmed training completion is tracked, and follow-ups are made for overdue staff on the compliance platform.<br>Observed security awareness training completion records demonstrating adherence to annual awareness training requirements on the Vanta compliance platform for all contractors and new hires during the observation period. | No Exception |
| **TSC ref # CC2.2.5** The Organization's information security policies and procedures are documented and reviewed at least annually. | Inspected the published security policies, revision histories, and approval records maintained within the Vanta compliance platform. Evidence reviewed showed that policy drafts are prepared by the Head of IT and subsequently reviewed and approved by the organization's relevant POC.<br>Conducted discussions with management regarding the policy governance process, including periodic reviews, updates, and approval responsibilities.<br>Validated through inspection of the compliance platform that current policy versions included documented revision histories, approval timestamps, and evidence of Head of IT and Co-Founder approval and were marked as active for the next review cycle. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC2.2.6** The Organization provides a description of its products and services to internal and external users. | Reviewed Fragment's MSA documentation, corporate website information, and summary materials outlining key offerings as services.<br>Interviews with the Head of IT and Co-Founder confirmed that interested parties are provided with the product descriptions.<br>Observed publicly available service descriptions on the company website (https://fragment.dev/products) and internal access to service materials. | No Exception |
| **TSC ref # CC2.2.7** The Organization communicates system changes to authorized internal users. | Reviewed change notifications, release notes, and operational communication procedures supporting system update visibility via emails and MS Teams channels by the Customer Success Manager.<br>Interviews confirmed that change communications are managed through established workflows prior to deployment.<br>Observed internal communication examples relating to system changes on Slack during 2025-2026. | No Exception |
| **TSC ref # CC2.2.8** The Organization has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. | Inspected Fragment's Human Resource Policy and Whistleblower Policy and supporting documentation describing confidential and anonymous reporting mechanisms available to personnel.<br>Conducted discussions with Head of IT and Co-Founder regarding leadership oversight of whistleblower reports and the process for investigating and addressing concerns raised by employees and contractors.<br>Validated through inspection that personnel have access to an anonymous reporting mechanism for submitting concerns. No whistleblower reports were recorded during the audit period. Management indicated that employees are encouraged to raise concerns directly with leadership, and an open and transparent culture supports escalation of issues without fear of retaliation. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC2.3.1** The Organization's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS). | Reviewed Master Service Agreements and Terms of Service outlining confidentiality, data protection, and platform security commitments.<br>Interviewed the Head of IT and Co-Founder and confirmed security requirements are communicated and agreed prior to service commencement.<br>Observed executed contract examples containing formal security obligations in the Master Services Agreement.<br>Observed evidence of publicly available terms and conditions. | No Exception |
| **TSC ref # CC2.3.2** The Organization provides guidelines and technical support resources relating to system operations to customers. | Reviewed customer onboarding materials, user manuals, troubleshooting instructions, and helpdesk support documentation.<br>Interviews with the Head of IT and Co-Founder confirmed availability and ongoing updates to support knowledge resources.<br>Observed accessible support content through the customer portal, Slack channels, and via email (i.e., help@fragment.dev). | No Exception |
| **TSC ref # CC2.3.3** The Organization provides a description of its products and services to internal and external users. | Reviewed Fragment's MSA documentation, corporate website information, and summary materials outlining key offerings as services.<br>Interviews with the Head of IT and Co-Founder confirmed that interested parties are provided with the product descriptions.<br>Observed publicly available service descriptions on the company website (https://fragment.dev/products) and internal access to service materials. | No Exception |

| | | |
|---|---|---|
| **TSC ref # CC2.3.4** The Organization has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. | Reviewed support ticketing system processes and escalation documentation.<br>Interviews with the Head of IT and Co-Founder confirmed that client issues are logged, triaged, and assigned to appropriate teams for resolution.<br>Observed operational communication channel on Slack and integrated Spot tool with tracking of support cases and response timelines. | No Exception |
| **TSC ref # CC2.3.5** The Organization notifies customers of critical system changes that may affect their processing. | Reviewed change communication procedures and customer update notifications for system releases or significant infrastructure changes.<br>Interviews with the Head of IT and Co-Founder confirmed that change summaries are sent to impacted customers ahead of deployment when applicable.<br>Observed sample customer communications regarding recent platform updates.<br>All the changes are communicated via Slack channels and via emails directly to the customers. Major product-related change information is also available on the organization's public website.<br>Change logs are available on the website (https://fragment.dev/changelog). | No Exception |
| **TSC ref # CC2.3.6** The Organization has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Reviewed executed vendor agreements including security, confidentiality, and data protection clauses governing the handling of company or customer information.<br>Interviews with the Head of IT and Co-Founder confirmed formal due diligence, and contracting is required before granting access to systems or data.<br>Observed monitored vendor contract records stored within the compliance platform for listed vendors (e.g., Vanta, GCP, Linear, Slack, and Certn). | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.3 Risk Assessment

| TSC ref # CC3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC3.1.1** The Organization specifies its objectives to enable the identification and assessment of risk related to the objectives. | Reviewed strategic and operational objectives documented in organizational plans, governance documentation, and departmental charters, identifying alignment with information security risk considerations.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that leadership establishes objectives that support risk identification and prioritization across business functions.<br><br>Observed weekly senior leadership meetings include discussions focused on performance against objectives and associated risk implications.<br><br>Leadership, including the founder and co-founder, discuss the operational risk and business objectives on a regular basis.<br><br>Evidence reviewed for these weekly and monthly discussions from the observation period. | No Exception |
| **TSC ref # CC3.1.2** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br><br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br><br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br><br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risks identified in the risk register currently available on the compliance platform. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC3.2.1** The Organization has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. | Reviewed the organization's Business Continuity and Disaster Recovery (BC/DR) Plan, including defined recovery responsibilities, communication procedures, recovery time objectives, and documented protocols for business service restoration. Also reviewed evidence of periodic BC/DR testing and resulting corrective action plans.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that BC/DR exercises are conducted at least annually, and lessons learned from tests are used to improve resiliency.<br><br>Observed evidence of recent BC/DR test results dated 07-May-2025, including test dates, scope, management approvals, and documented follow-up activities to address identified gaps.<br><br>A DDoS Attack scenario was presented for discussion and to gauge preparedness during the tabletop exercise. | No Exception |
| **TSC ref # CC3.2.2** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br><br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br><br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br><br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risks identified in the risk register currently available on the compliance platform. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC3.2.3** The Organization's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Reviewed Fragment's Risk Assessment documentation covering environmental, regulatory, and technological changes that could affect security commitments and objectives. Evidence included annual risk assessment reports and updates to controls based on identified risk.<br>Interviews with the Head of IT and Co-Founder confirmed that leadership incorporates fraud considerations into the annual risk assessment process and evaluates the likelihood and impact of fraud-related risks.<br>Observed documented results of the most recent annual risk assessment, including action plans for identified risks and review acknowledgment from senior management.<br>Reviewed the Risk snapshot on Vanta dated 09-Feb-2026, with a total of 10 Risks Identified. | No Exception |
| **TSC ref # CC3.2.4** The Organization has a vendor management program in place. Components of this program include:<br>▪ critical third-party vendor inventory;<br>▪ vendor's security and privacy requirements; and<br>▪ review of critical third-party vendors at least annually. | Reviewed the vendor management policy and third-party inventory identifying critical suppliers, along with contracts defining security and confidentiality requirements.<br>Interviews with the Head of IT and Co-Founder verified that vendor oversight responsibilities include periodic review of vendor performance and security posture, with results reported to management.<br>Observed evidence of an annual vendor review process including assessment of security documentation, compliance confirmations, and contractual obligations.<br>Observed the security reviews completed for all the critical, high, medium and low vendors by the Head of IT and relevant POCs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC3.3.1** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risks identified in the risk register currently available on the compliance platform. | No Exception |
| **TSC ref # CC3.3.2** The Organization's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Reviewed Fragment's Risk Assessment documentation covering environmental, regulatory, and technological changes that could affect security commitments and objectives. Evidence included annual risk assessment reports and updates to controls based on identified risk.<br>Interviews with the Head of IT and Co-Founder confirmed that leadership incorporates fraud considerations into the annual risk assessment process and evaluates the likelihood and impact of fraud-related risks.<br>Observed documented results of the most recent annual risk assessment, including action plans for identified risks and review acknowledgment from senior management.<br>Reviewed the Risk snapshot on Vanta dated 09-Feb-2026, with a total of 10 Risks identified. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC3.4 - The entity identifies and assesses changes that could significantly impact the system of internal control. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC3.4.1** The Organization has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. | Observed that system configurations are defined and managed through Infrastructure-as-Code and deployed via automated CI/CD pipelines, ensuring consistency across all environments and AWS regions. Observed that AWS Control Tower and AWS Organizations provide centralized governance and account-level standardization. Configuration changes are controlled through GitHub pull requests requiring peer review and automated validation before deployment to production.<br><br>Interviewed the Head of IT who confirmed that all infrastructure and application configurations are deployed through standardized CI pipelines and that manual configuration changes in production environments are restricted. They further confirmed that Seed CI system enforces consistent environment provisioning and deployment controls.<br><br>Based on the procedures performed, configuration management practices are operating effectively and ensure consistent deployment of system configurations across the environment. No exceptions were noted. | No Exception |
| **TSC ref # CC3.4.2** The Organization's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs. | Reviewed Fragment's Operational Security Policy; a penetration test is conducted annually.<br><br>Interviewed the Head of IT and Co-Founder and confirmed a penetration test was conducted by CL, dated 06-Mar-2026. Three Medium-level vulnerabilities were identified.<br><br>The organization presented the remediations of these vulnerabilities. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC3.4.3** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br><br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br><br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br><br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risk identified in the risk register currently available in the compliance platform. | No Exception |
| **TSC ref # CC3.4.4** The Organization's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Reviewed Fragment's Risk assessment documentation covering environmental, regulatory, and technological changes that could affect security commitments and objectives. Evidence included annual risk assessment reports and updates to controls based on identified risk.<br><br>Interviews with the Head of IT and Co-Founder confirmed that leadership incorporates fraud considerations into the annual risk assessment process and evaluates the likelihood and impact of fraud-related risks.<br><br>Observed documented results of the most recent annual risk assessment, including action plans for identified risks and review acknowledgment from senior management.<br><br>Reviewed the Risk snapshot on Vanta dated 09-Feb-2026, with a total of 10 Risks identified. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.4 Monitoring Activities

| TSC ref # CC4.1 - The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC4.1.1** The Organization performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the Organization has committed to an SLA for a finding, the corrective action is completed within that SLA. | Reviewed Fragment's Operational Security Policy and annual internal control self-assessment documentation, corrective action tracking logs, and remediation tracking procedures outlining timelines and SLA compliance.<br>Interviewed the Head of IT and Co-Founder and confirmed that senior leadership oversees control assessments and remediation progress through structured review meetings on a weekly basis.<br>Observed completed control assessment reports and evidence of open and closed remediation tasks tracked to completion within agreed timelines.<br>Reviewed the external penetration test reports and remediation actions.<br>The organization also relies on the Vanta compliance platform for security posture assessment through implemented controls. | No Exception |
| **TSC ref # CC4.1.2** The Organization's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs. | Reviewed Fragment's Operational Security Policy; the penetration test is conducted annually.<br>Interviewed the Head of IT and Co-Founder and confirmed a penetration test was conducted by CL, dated 06-Mar-2026. Three Medium-level vulnerabilities were identified.<br>The organization presented the remediations of these vulnerabilities. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC4.1.3** The Organization has a vendor management program in place. Components of this program include:<br>▪ critical third-party vendor inventory;<br>▪ vendor's security and privacy requirements; and<br>▪ review of critical third-party vendors at least annually. | Reviewed the vendor management policy and third-party inventory identifying critical suppliers, along with contracts defining security and confidentiality requirements.<br>Interviews with the Head of IT and Co-Founder verified that vendor oversight responsibilities include periodic review of vendor performance and security posture, with results reported to management.<br>Observed evidence of an annual vendor review process including assessment of security documentation, compliance confirmations, and contractual obligations.<br>Observed the security reviews completed for all the critical, high, medium and low vendors by the Head of IT and relevant POCs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC4.1.4** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC4.2 - The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC4.2.1** The Organization performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the Organization has committed to an SLA for a finding, the corrective action is completed within that SLA. | Reviewed Fragment's Operational Security Policy and annual internal control self-assessment documentation, corrective action tracking logs, and remediation tracking procedures outlining timelines and SLA compliance.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that senior leadership oversees control assessments and remediation progress through structured review meetings on a weekly basis.<br><br>Observed completed control assessment reports and evidence of open and closed remediation tasks tracked to completion within agreed timelines.<br><br>Reviewed the external penetration test reports and remediation actions.<br><br>The organization is also relying on Vanta compliance platform for security posture assessment through implemented controls. | No Exception |
| **TSC ref # CC4.2.2** The Organization has a vendor management program in place. Components of this program include:<br>▪ critical third-party vendor inventory;<br>▪ vendor's security and privacy requirements; and<br>▪ review of critical third-party vendors at least annually. | Reviewed the vendor management policy and third-party inventory identifying critical suppliers, along with contracts defining security and confidentiality requirements.<br><br>Interviews with the Head of IT and Co-Founder verified that vendor oversight responsibilities include periodic review of vendor performance and security posture, with results reported to management.<br><br>Observed evidence of an annual vendor review process including assessment of security documentation, compliance confirmations, and contractual obligations.<br><br>Observed the security reviews completed for all the critical, high, medium and low vendors by the Head of IT and relevant POCs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.5 Control Activities

| TSC ref # CC5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC5.1.1** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risks identified in the risk register currently available on the compliance platform. | No Exception |
| **TSC ref # CC5.1.2** The Organization's information security policies and procedures are documented and reviewed at least annually. | Inspected the published security policies, revision histories, and approval records maintained within the Vanta compliance platform. Evidence reviewed showed that policy drafts are prepared by the Head of IT and subsequently reviewed and approved by the organization's relevant POC.<br>Conducted discussions with management regarding the policy governance process, including periodic reviews, updates, and approval responsibilities.<br>Validated through inspection of the compliance platform that current policy versions included documented revision histories, approval timestamps, and evidence of Head of IT and Co-Founder approval and were marked as active for the next review cycle. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC 5.2.1** The Organization's access control policy documents the requirements for the following access control functions:<br>▪ Adding new users<br>▪ Modifying users;<br>▪ Removing user access | Reviewed Fragment's Access Control Policy, including documented procedures for new user provisioning, role or responsibility-based access modifications, and timely access removal upon termination or role changes.<br>Interviewed the Head of IT and Co-Founder and confirmed adherence to documented processes and the use of approval workflows to ensure appropriate access assignment.<br>Observed examples of user access records and onboarding (PM)/offboarding (MA) evidence demonstrating implementation of approved access control procedures. | No Exception |
| **TSC ref # CC 5.2.2** The Organization has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Reviewed SDLC documentation outlining structured processes for system development and changes, including requirements gathering, testing, approvals, and controlled deployment processes for production changes.<br>Interviewed the Head of IT and Co-Founder and confirmed that the SDLC is actively followed for enhancements and new system implementations, including emergency change handling.<br>Observed evidence of change records with testing artifacts and approval documentation supporting compliance with the SDLC methodology.<br>Reviewed GitHub and KanBan for project management of the active and completed requirements. Daily Standup meetings are held for the review of the ongoing developments.<br>GitHub Advanced Security is used; Linear is used for software developments.<br>Development evidence reviewed for FRA-7079, 6938, & 6922. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC 5.2.3** The Organization's information security policies and procedures are documented and reviewed at least annually. | Inspected the published security policies, revision histories, and approval records maintained within the Vanta compliance platform. Evidence reviewed showed that policy drafts are prepared by the Head of IT and subsequently reviewed and approved by the organization's relevant POC.<br><br>Conducted discussions with management regarding the policy governance process, including periodic reviews, updates, and approval responsibilities.<br><br>Validated through inspection of the compliance platform that current policy versions included documented revision histories, approval timestamps, and evidence of Head of IT and Co-Founder approval and were marked as active for the next review cycle. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC5.3.1** The Organization's data backup policy documents requirements for backup and recovery of customer data. | Reviewed the Data Backup and Recovery Policy outlining backup schedules, storage requirements, and recovery processes to ensure data availability.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that backup policies are centrally defined and enforced through AWS-native services, and that no manual backup processes are used in production environments. They further confirmed that backup and recovery requirements are applied consistently across all in-scope systems and regions.<br><br>Observed that the organization leverages AWS-native backup and storage services to implement automated and policy-driven backup processes. DynamoDB data is maintained in multiple internal copies, with an additional copy exported to Amazon S3 within the same region to support redundancy. AWS Backup is configured to manage scheduled backups and ensure consistency across production systems.<br><br>Observed that backups are replicated across multiple AWS regions to support disaster recovery objectives. Management confirmed that cross-region backup retention supports an RPO of three days for recovery scenarios requiring regional failover.<br><br>Observed that the organization has implemented a multi-region infrastructure architecture spanning North America, Europe, and Asia-Pacific regions. Production workloads are distributed across AWS regions US-East-1, US-East-2, US-West-2, AP-Southeast-2 (Sydney), EU-Frankfurt, and EU-Ireland, providing geographic redundancy and resilience. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC5.3.2** The Organization requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Reviewed change management procedures requiring change requests, impact assessments, testing, approval, and implementation tracking.<br>Interviewed the Head of IT and Co-Founder and confirmed consistent enforcement of the change review and approval process.<br>There were no activities or changes on the infrastructure within the observation period. Although, changes related to the core software were observed and found satisfactory. | No Exception |
| **TSC ref # CC5.3.3** The Organization has formal retention and disposal procedures in place to guide the secure retention and disposal of Organization and customer data. | Reviewed documented data retention and secure disposal procedures specifying data handling timelines and destruction methods.<br>Interviewed the Head of IT and Co-Founder and confirmed adherence to retention schedules and approved disposal workflows.<br>Observed policy-driven controls for secure deletion and disposal of sensitive information and media.<br>- Alt***t was offboarded in Mar-2026, and Ka*D in Apr-2026. | No Exception |
| **TSC ref # CC5.3.4** The Organization has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Reviewed SDLC documentation outlining structured processes for system development and changes, including requirements gathering, testing, approvals, and controlled deployment processes for production changes.<br>Interviewed the Head of IT and Co-Founder and confirmed that the SDLC is actively followed for enhancements and new system implementations, including emergency change handling.<br>Observed evidence of change records with testing artifacts and approval documentation supporting compliance with the SDLC methodology.<br>Reviewed GitHub and KanBan for project management of the active and completed requirements. Daily Standup meetings are held for the review of the ongoing developments.<br>GitHub Advanced Security is used; Linear is used for software developments.<br>Development evidence reviewed for FRA-7079, 6938, & 6922. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC5.3.5** The Organization has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Reviewed incident response policies, incident reporting workflows, and communication protocols that define how personnel must report and respond to cybersecurity and privacy incidents.<br>Interviewed the Head of IT and Co-Founder and confirmed that employees are informed of reporting channels and escalation expectations during onboarding and refresher training.<br>Observed access to incident response documentation on internal platforms (i.e. Slack).<br>Reviewed the one incident related to the service downtime<br>The incident management platform Incident.io is used for incident tracking. | No Exception |
| **TSC ref # CC5.3.6** The Organization specifies its objectives to enable the identification and assessment of risk related to the objectives. | Reviewed strategic and operational objectives documented in organizational plans, governance documentation, and departmental charters, identifying alignment with information security risk considerations.<br>Interviewed the Head of IT and Co-Founder and confirmed that leadership establishes objectives that support risk identification and prioritization across business functions.<br>Observed the weekly senior leadership meetings include discussions focused on performance against objectives and associated risk implications.<br>Leadership, including founder and co-founder, discuss the operational risk and business objectives on regular basis.<br>Evidence was reviewed for these weekly and monthly discussions from the observation period. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC5.3.7** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br><br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br><br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br><br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risks identified in the risk register currently available on the compliance platform. | No Exception |
| **TSC ref # CC5.3.8** Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Reviewed the information security job roles and responsibilities documents along with the organizational chart defining responsibilities for managing information security controls throughout the technology environment lifecycle.<br><br>Interviewed the Head of IT and Co-Founder and confirmed staff responsibilities are assigned and communicated during onboarding and role transitions.<br><br>Reviewed the job descriptions for Head of IT, Head of Engineering, Engineering Team, and Designers.<br><br>Observed evidence of documented job responsibilities and acknowledgment supporting accountability for security-related duties. | No Exception |
| **TSC ref # CC5.3.9** The Organization's information security policies and procedures are documented and reviewed at least annually. | Inspected the published security policies, revision histories, and approval records maintained within the Vanta compliance platform. Evidence reviewed showed that policy drafts are prepared by the Head of IT and subsequently reviewed and approved by the organization's relevant POC.<br><br>Conducted discussions with management regarding the policy governance process, including periodic reviews, updates, and approval responsibilities.<br><br>Validated through inspection of the compliance platform that current policy versions included documented revision histories, approval timestamps, and evidence of Head of IT and Co-Founder approval and were marked as active for the next review cycle. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC5.3.10** The Organization has a vendor management program in place. Components of this program include:<br>▪ critical third-party vendor inventory;<br>▪ vendor's security and privacy requirements; and<br>▪ review of critical third-party vendors at least annually. | Reviewed the vendor management policy and third-party inventory identifying critical suppliers, along with contracts defining security and confidentiality requirements.<br>Interviews with the Head of IT and Co-Founder verified that vendor oversight responsibilities include periodic review of vendor performance and security posture, with results reported to management.<br>Observed evidence of an annual vendor review process including assessment of security documentation, compliance confirmations, and contractual obligations.<br>Observed the security reviews completed for all the critical, high, medium and low vendors by the Head of IT and relevant POCs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.6 Logical and Physical Access Controls

| TSC ref # CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.1.1** The Organization's access control policy documents the requirements for the following access control functions:<br>▪ adding new users;<br>▪ modifying users; and/or<br>▪ removing an existing user's access. | Reviewed Fragment's Access Control Policy, including documented procedures for new user provisioning, role or responsibility-based access modifications, and timely access removal upon termination or role changes.<br>Interviewed the Head of IT and Co-Founder and confirmed adherence to documented processes and the use of approval workflows to ensure appropriate access assignment.<br>Observed examples of user access records and onboarding (PM)/offboarding (MA) evidence demonstrating implementation of approved access control procedures. | No Exception |
| **TSC ref # CC6.1.2** The Organization ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Reviewed onboarding and access approval procedures demonstrating that role-based access is assigned according to job responsibilities and requires management approval prior to provisioning.<br>Interviewed the Head of IT and Co-Founder and confirmed that new access requests are reviewed and approved by the hiring manager to ensure alignment with "least privilege" principles.<br>Observed recent access request tickets for employee PM that included documented approvals supporting adherence to role-based access requirements. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.1.3** The Organization has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | Reviewed Fragment's Data Management Policy outlining data sensitivity tiers and corresponding handling, storage, and access protection requirements.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that classification requirements are communicated to employees and used to determine appropriate safeguards for confidential data.<br><br>Observed implementation of data labeling and restricted access to systems containing sensitive information aligned with the Data Classification Policy.<br><br>The organization has defined Personal, Sensitive, Confidential Customer Data, Confidential Internal, Restricted, and Public Data classifications and labelling for only paper records when they are needed. | No Exception |
| **TSC ref # CC6.1.4** The Organization's data stores housing sensitive customer data are encrypted at rest. | Reviewed system security configurations and encryption standards indicating that sensitive customer data stored within production data stores is encrypted at rest.<br><br>Interviewed the Head of IT and Co-Founder and confirmed the use of industry-accepted encryption protocols and periodic validation of encryption settings.<br><br>Observed evidence within system configuration dashboards and technical documentation showing encryption is enabled for data repositories storing sensitive information.<br><br>AES-256 encryption protocols are implemented.<br>AWS, TLS-1.2 or higher is used for data in transit. | No Exception |
| **TSC ref # CC6.1.5** The Organization restricts privileged access to encryption keys to authorized users with a business need. | Reviewed key management procedures and access control lists indicating privileged access to encryption keys is limited to authorized personnel.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that key access is tightly controlled and periodically reviewed to ensure continued alignment with business needs.<br><br>Observed restricted access settings within the key management environment and audit logs supporting controlled access. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.1.6** The Organization restricts privileged access to the firewall to authorized users with a business need. | Reviewed the Operational Security policy and procedure and access role documentation supporting restricted assignment of Network configuration privileges.<br><br>Interviewed the Head of IT and Co-Founder and confirmed only qualified personnel are authorized to modify firewall rules. The organization is using AWS WAF.<br><br>Observed Network access permissions demonstrating limited administrative access. | No Exception |
| **TSC ref # CC6.1.7** The Organization's network is segmented to prevent unauthorized access to customer data. | Reviewed network diagrams and segmentation policies describing logical separation of environments handling sensitive data.<br><br>Interviewed the Head of IT and Co-Founder and confirmed segmentation controls are designed to restrict access paths to customer information.<br><br>Observed Fragment's infrastructure is deployed on AWS, segmented through AWS-native controls to prevent unauthorized access to customer data. As observed through the network architecture diagram, all inbound traffic from external clients — Fragment Dashboard and Customer Backend — is routed exclusively through AWS API Gateway, serving as the sole entry point, with no direct external access to internal services such as Lambda, DynamoDB, Elastic, SQS, or EventBridge. AWS Organizations and Control Tower enforce account-level segmentation and governance guardrails across the environment. The infrastructure is independently deployed across 6 AWS regions (US-East-1, US-East-2, US-West-2, AP-Southeast-2, EU-Frankfurt, EU-Ireland), each across 3 Availability Zones. Network activity is monitored via AWS CloudTrail, GuardDuty (alerts integrated with Slack), and Elastic, with logs retained for 13 months. | No Exception |

| | | |
|---|---|---|
| **TSC ref # CC6.1.8** The Organization requires passwords for in-scope system components to be configured according to the Organization's policy. | Reviewed password policy outlining complexity, expiration, and lockout requirements enforced across applications and infrastructure.<br><br>Interviewed the Head of IT and Co-Founder and confirmed password standards are applied and monitored routinely.<br><br>Observed Fragment's in-scope system components are hosted on AWS, with access governed through AWS Organizations and Control Tower, enforcing consistent access policies across all environments. Privileged access to system components is requested via Slack, ensuring access is tracked and approved before being granted. As confirmed during the interview with the Head of IT and Co-Founder, an active Cybersecurity Policy is in place governing password and access requirements across in-scope systems. | No Exception |
| **TSC ref # CC6.1.9** System access restricted to authorized access only | Reviewed access control policies and provisioning procedures defining roles, approvals, and authentication mechanisms for system access.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that unauthorized access attempts are monitored and investigated.<br><br>The organization is using AWS GuardDuty for monitoring and as an IDS.<br><br>Observed that Fragment restricts system access through AWS Organizations and Control Tower, enforcing access governance across all environments. Privileged access is requested via Slack, ensuring access is approved before being granted. As observed, new joiner PM was onboarded on 29-Jan-2026 with access provisioned accordingly; and for leaver MA, access was revoked upon his last working day (03-Apr-2026), with the offboarding checklist reviewed as evidence. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.1.10** The Organization restricts privileged access to databases to authorized users with a business need. | Reviewed database access management procedures and privileged role documentation confirming business justification requirements.<br><br>Interviewed the Head of IT and Co-Founder and confirmed periodic reviews occur for elevated access to database environments.<br><br>Observed that Fragment's primary database, AWS DynamoDB, is hosted within the AWS environment and is not directly accessible from any external client. As observed in the network architecture, DynamoDB is only reachable internally via AWS Lambda, ensuring no direct public access. Privileged access to the database is requested through Slack, requiring approval prior to access being granted, ensuring access is tied to a business need. | No Exception |
| **TSC ref # CC6.1.11** The Organization restricts access to migrate changes to production to authorized personnel. | Reviewed change management procedures requiring authorization, peer validation, and approvals before deployment to production.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that only specified personnel can deploy production changes.<br><br>Observed change deployment logs showing restricted execution of migration activities.<br><br>Access is limited to the Engineering team’s specific admin only. | No Exception |
| **TSC ref # CC6.1.12** The Organization maintains a formal inventory of production system assets. | Reviewed asset inventory documentation containing system components, ownership information, and tracking details.<br><br>Interviewed the Head of IT and Co-Founder and confirmed the inventory is maintained and reviewed regularly to ensure accuracy on the Vanta compliance platform.<br><br>Observed inventory management tool reports confirming completeness of system assets.<br><br>Endpoint inventory is maintained on Vanta via Vanta MDM agent. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.1.13** The Organization restricts privileged access to the production network to authorized users with a business need. | Reviewed network access control procedures and permissions for production environment connectivity.<br><br>Interviewed the Head of IT and Co-Founder and confirmed privileged production access is granted only based on operational need.<br><br>Observed that Fragment's Infrastructure is managed entirely as Infrastructure as Code (IaC), deployed through a CI system called Seed, ensuring production network changes are version-controlled and go through a peer-reviewed, automated deployment process rather than direct manual access. Privileged access to the production network is requested via Slack, ensuring access is approved and tied to a business need prior to being granted. | No Exception |
| **TSC ref # CC6.1.14** The Organization's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | Reviewed the secure remote access policy and technical controls.<br><br>Interviewed the Head of IT and Co-Founder and confirmed enforcement of approved secure remote access methods.<br><br>Observed all inbound traffic routed exclusively through AWS API Gateway, ensuring no direct exposure of internal services to the public internet. Access to the production environment is governed through AWS Organizations and Control Tower, with privileged access requests made via Slack and approved prior to being granted. Infrastructure is managed as Infrastructure as Code (IaC) and deployed through the Seed CI system, limiting the need for direct human access to production systems. It was noted during the interview that the Organization does not utilize a VPN for remote access to production systems. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.1.15** The Organization's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. | Reviewed the MFA policy and enrollment requirements for privileged and remote system access.<br><br>Interviewed the Head of IT and Co-Founder and confirmed mandatory MFA usage for remote production access.<br><br>Observed authentication logs requiring MFA validation before establishing remote sessions.<br><br>As confirmed during the interview with the Head of IT and Co-Founder, the organization does not use VPN or SSH for remote access to production systems. Instead, access is enforced through MFA, ensuring only authorized employees with a valid MFA method can access production systems. | No Exception |
| **TSC ref # CC6.1.16** The Organization requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys. | Interviewed the Head of IT and Co-Founder and confirmed enforcement of unique identity for accountability.<br><br>Discussed during the interview with the Head of IT and Co-Founder, Fragment does not utilize SSH keys for authentication to systems and applications. Authentication is enforced through unique username and password credentials, supplemented by MFA, across in-scope systems and applications. Access to the production environment is governed through AWS Organizations and Control Tower, with privileged access requests made via Slack and approved prior to being granted. | No Exception |
| **TSC ref # CC6.1.17** The Organization requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | Reviewed documentation confirming unique account and secure credential requirements for production network authentication.<br><br>Interviewed the Head of IT and Co-Founder and validated enforcement of strong authentication controls.<br><br>Discussed during the interview with the Head of IT and Co-Founder, Fragment does not utilize SSH keys for authentication to the production network. Authentication to the production network is enforced through unique username and password credentials, supplemented by MFA, governed through AWS Organizations and Control Tower across all 06 production regions. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.1.18** The Organization requires authentication to production data stores to use authorized secure authentication mechanisms, such as unique SSH key. | Reviewed Fragment's Operational Security policy and database security standards requiring secure authentication (e.g., SSH keys) and accountability for access.<br><br>Interviewed the Head of IT and Co-Founder and confirmed enforcement of secure data store authentication practices.<br><br>As observed in the network architecture, Fragment's production data stores — AWS DynamoDB and AWS S3 — are not publicly accessible. Authentication to these data stores is handled internally within the AWS environment, where AWS Lambda is the only service with direct access to DynamoDB, and DynamoDB exports to S3 through an internal, controlled pipeline. As confirmed during the interview, Fragment does not utilize SSH keys for data store authentication, instead relying on AWS-native authentication mechanisms through IAM roles and policies, governed by AWS Organizations and Control Tower, ensuring only authorized services and users can authenticate to production data stores. | No Exception |
| **TSC ref # CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity user system credential are removed when user access is no longer authorized.** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.2.1** The Organization's access control policy documents the requirements for the following access control functions:<br>▪ adding new users;<br>▪ modifying users; and/or<br>▪ removing an existing user's access. | Reviewed Fragment's Access Control Policy, including documented procedures for new user provisioning, role or responsibility-based access modifications, and timely access removal upon termination or role changes.<br><br>Interviewed the Head of IT and Co-Founder and confirmed adherence to documented processes and the use of approval workflows to ensure appropriate access assignment.<br><br>Observed examples of user access records and onboarding (PM)/offboarding (MA) evidence demonstrating implementation of approved access control procedures. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.2.2** The Organization ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Reviewed onboarding and access approval procedures demonstrating that role-based access is assigned according to job responsibilities and requires management approval prior to provisioning.<br>Interviewed the Head of IT and Co-Founder and confirmed that new access requests are reviewed and approved by the hiring manager to ensure alignment with least privilege principles.<br>Observed recent access request tickets to Employee (PM) that included documented approvals supporting adherence to role-based access requirements. | No Exception |
| **TSC ref # CC6.2.3** The Organization conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. | Reviewed the Access Control policy, which specifies the access rights review is to be conducted on a quarterly basis.<br>Interview the Head of IT and Co-Founder and discussed the review process. | **Exception Noted:**<br>An access rights review was not found for this current year; the last one was conducted 30-Jan-2025. |
| **TSC ref # CC6.2.4** The Organization completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Reviewed Access Control policy and offboarding workflow documentation, including termination checklists and system access deactivation records.<br>Interviewed the Head of IT and Co-Founder and confirmed that access removal timelines follow internal SLAs.<br>Observed access removal tickets demonstrating timely revocation for terminated personnel.<br>Reviewed the same-day access revocation for offboarded user MA, leaving date 03-Apr-2026. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.2.5** The Organization requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys. | Interviewed the Head of IT and Co-Founder and confirmed enforcement of unique identity for accountability.<br><br>Discussed during the interview with the Head of IT and Co-Founder, Fragment does not utilize SSH keys for authentication to systems and applications. Authentication is enforced through unique username and password credentials, supplemented by MFA, across in-scope systems and applications. Access to the production environment is governed through AWS Organizations and Control Tower, with privileged access requests made via Slack and approved prior to being granted. | No Exception |
| **TSC ref # CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.3.1** The Organization's access control policy documents the requirements for the following access control functions:<br>▪ adding new users;<br>▪ modifying users; and/or<br>▪ removing an existing user's access. | Reviewed Fragment's Access Control Policy, including documented procedures for new user provisioning, role or responsibility-based access modifications, and timely access removal upon termination or role changes.<br><br>Interviewed the Head of IT and Co-Founder and confirmed adherence to documented processes and the use of approval workflows to ensure appropriate access assignment.<br><br>Observed examples of user access records and onboarding (PM)/offboarding (MA) evidence demonstrating implementation of approved access control procedures. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.3.2** The Organization ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Reviewed onboarding and access approval procedures demonstrating that role-based access is assigned according to job responsibilities and requires management approval prior to provisioning.<br>Interviewed the Head of IT and Co-Founder and confirmed that new access requests are reviewed and approved by the hiring manager to ensure alignment with "least privilege" principles.<br>Observed recent access request tickets for employee PM that included documented approvals supporting adherence to role-based access requirements. | No Exception |
| **TSC ref # CC6.3.3** The Organization conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. | Reviewed the Access Control policy, which specifies the access rights review is to be conducted on a quarterly basis.<br>Interview the Head of IT and Co-Founder and discussed the review process. | **Exception Noted:**<br>See **TSC ref # CC6.2.3** |
| **TSC ref # CC6.3.4** The Organization completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Reviewed Access Control policy and offboarding workflow documentation, including termination checklists and system access deactivation records.<br>Interviewed the Head of IT and Co-Founder and confirmed that access removal timelines follow internal SLAs.<br>Observed access removal tickets demonstrating timely revocation for terminated personnel.<br>Reviewed the same-day access revocation for offboarded user MA, leaving date 03-Apr-2026. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.3.5** The Organization requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys. | Interviewed the Head of IT and Co-Founder and confirmed enforcement of unique identity for accountability.<br><br>Discussed during the interview with the Head of IT and Co-Founder, Fragment does not utilize SSH keys for authentication to systems and applications. Authentication is enforced through unique username and password credentials, supplemented by MFA, across in-scope systems and applications. Access to the production environment is governed through AWS Organizations and Control Tower, with privileged access requests made via Slack and approved prior to being granted. | No Exception |
| **TSC ref # CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel.** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.4.1** The Organization conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. | The organization's infrastructure is hosted within a cloud-based environment and relies on designated subservice providers for the implementation and operation of this control. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.5.1** The Organization completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Reviewed Access Control policy and offboarding workflow documentation, including termination checklists and system access deactivation records.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that access removal timelines follow internal SLAs.<br><br>Observed access removal tickets demonstrating timely revocation for terminated personnel.<br><br>Reviewed the same-day access revocation for offboarded user MA, leaving date 03-Apr-2026. | No Exception |
| **TSC ref # CC6.5.2** The Organization has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. | Inspected the Data Management Policy, which requires data classified as Restricted or Confidential to be securely deleted when no longer needed and requires the organization to assess third-party data disposal practices in accordance with the Third-Party Management Policy.<br><br>Conducted discussions with the Head of IT and Co-Founder regarding procedures for secure deletion of information and the evaluation of third-party service providers' data destruction controls.<br><br>Validated through inspection that formal requirements for secure media purging and third-party data destruction have been established. No data purging or destruction events occurred during the audit period; therefore, no execution records were available for testing. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.5.3** The Organization purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. | Reviewed offboarding procedures requiring that customer data is securely deleted or extracted at contract termination per documented guidelines.<br>Interviewed the Head of IT and Co-Founder and confirmed customers are notified of data retention timeframes, and deletion is tracked to completion.<br>No customer Data Deletion requests were received during the observation period. | No Exception |
| **TSC ref # CC6.5.4** The Organization has formal retention and disposal procedures in place to guide the secure retention and disposal of Organization and customer data. | Reviewed documented data retention and secure disposal procedures specifying data handling timelines and destruction methods.<br>Interviewed the Head of IT and Co-Founder and confirmed adherence to retention schedules and approved disposal workflows.<br>Observed policy-driven controls for secure deletion and disposal of sensitive information and media.<br>- Alt***t was offboarded in March 2026, and Ka*D in April 2026. | No Exception |
| **TSC ref # CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.6.1** The Organization uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Reviewed policies and configuration settings requiring encryption (e.g., TLS 1.2) for transmitting sensitive data across public networks.<br>Interviewed the Head of IT and Co-Founder and confirmed encryption enforcement through network security controls.<br>Observed active TLS configurations and data flow diagrams showing encrypted transmission pathways. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.6.2** The Organization uses an intrusion detection system to provide continuous monitoring of the Organization's network and early detection of potential security breaches. | Reviewed AWS IDS configuration documentation showing continuous monitoring and alerting capabilities.<br><br>Interviewed the Head of IT and Co-Founder and confirmed security operations review alerts and perform incident response actions.<br><br>Observed AWS GuardDuty dashboard screens and historical alert logs demonstrating active monitoring.<br>The notifications and alerts on IDS are instantly taken up by the Engineering team. | No Exception |
| **TSC ref # CC6.6.3** The Organization's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. | Reviewed documented hardening guidelines derived from industry standards with annual review evidence.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that infrastructure is deployed and maintained per defined security standards.<br><br>Observed Fragment's network and system hardening is enforced through AWS Organizations and Control Tower, applying consistent security guardrails across all environments based on AWS industry best practices. Infrastructure is managed entirely as Infrastructure as Code (IaC), ensuring all system configurations are documented, version-controlled, and consistently applied across all environments. AWS CloudTrail and GuardDuty provide continuous monitoring against hardening standards, with alerts integrated into Slack. | No Exception |

| | | |
|---|---|---|
| **TSC ref # CC6.6.4** The Organization reviews its firewall rulesets at least annually. Required changes are tracked to completion. | Reviewed firewall review procedures and annual review reports that track rule changes to resolution.<br><br>Interviewed the Head of IT and Co-Founder and confirmed periodic validation of rule relevance and removal of unused rules.<br><br>Observed Fragment's infrastructure does not rely on traditional firewalls. As observed in the network architecture, network access controls are enforced through AWS API Gateway as the sole entry point, with AWS Organizations and Control Tower governing security policies across all environments. Infrastructure is managed as Infrastructure as Code (IaC) and deployed through the Seed CI system, ensuring any changes to network access rules are version-controlled and peer-reviewed. | No Exception |
| **TSC ref # CC6.6.5** The Organization's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | Reviewed the Secure Remote Access policy and technical controls.<br><br>Interviewed the Head of IT and Co-Founder and confirmed enforcement of approved secure remote access methods.<br><br>Fragment's production systems are hosted on AWS across 06 regions, with all inbound traffic routed exclusively through AWS API Gateway, ensuring no direct exposure of internal services to the public internet. Access to the production environment is governed through AWS Organizations and Control Tower, with privileged access requests made via Slack and approved prior to being granted. Infrastructure is managed as Infrastructure as Code (IaC) and deployed through the Seed CI system, limiting the need for direct human access to production systems. It was noted during the interview that the organization does not utilize a VPN for remote access to production systems. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.6.6** The Organization's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. | Reviewed the MFA policy and enrollment requirements for privileged and remote system access.<br>Interviewed the Head of IT and Co-Founder and confirmed mandatory MFA usage for remote production access.<br>Observed authentication logs requiring MFA validation before establishing remote sessions.<br>As confirmed during the interview with the Head of IT and Co-Founder, the organization does not use VPN or SSH for remote access to production systems. Instead, access is enforced through MFA, ensuring only authorized employees with a valid MFA method can access production systems. | No Exception |
| **TSC ref # CC6.6.7** The Organization has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Reviewed Fragment's vulnerability management and patching procedures showing scheduled updates and remediation based on risk.<br>Interviewed the Head of IT and Co-Founder and confirmed timely patching aligned with industry best practices and SLAs.<br>Observed patch deployment logs and reports confirming recent updates applied across in-scope systems.<br>AWS CloudTrail is enabled by the organization and integrated into the compliance platform.<br>GuardDuty alerts are integrated with Slack.<br>GitHub is used for vulnerability management, with Dependabot integrated for any CVEs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.6.8** The Organization requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys. | Interviewed the Head of IT and Co-Founder and confirmed enforcement of unique identity for accountability.<br><br>As confirmed during the interview with the Head of IT and Co-Founder, Fragment does not utilize SSH keys for authentication to systems and applications. Authentication is enforced through unique username and password credentials, supplemented by MFA, across in-scope systems and applications. Access to the production environment is governed through AWS Organizations and Control Tower, with privileged access requests made via Slack and approved prior to being granted. | No Exception |
| **TSC ref # 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.** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.7.1** The Organization uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Reviewed policies and configuration settings requiring encryption (e.g., TLS 1.2) for transmitting sensitive data across public networks.<br><br>Interviewed the Head of IT and Co-Founder and confirmed encryption enforcement through network security controls.<br><br>Observed active TLS configurations and data flow diagrams showing encrypted transmission pathways. | No Exception |
| **TSC ref # CC6.7.2** The Organization has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. | Reviewed MDM deployment documentation including device enrollment, configuration enforcement, and remote wipe capabilities.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that only authorized, MDM-enrolled devices may access corporate resources.<br><br>Observed the Vanta agent console showing real-time compliance status, policy application, and the ability to restrict app and data usage on mobile devices. | **Exception Noted:**<br><br>The organization has not implemented a formal conventional MDM solution for centralized controlling of the user endpoint devices. |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.7.3** The Organization encrypts portable and removable media devices when used. | Reviewed procedures for securing portable and removable storage media, including mandatory encryption requirements.<br>Interviewed the Head of IT and Co-Founder and confirmed adherence to removable media encryption policies and restrictions on unauthorized usage.<br>Observed encryption enforcement settings on removable media devices and monitoring logs validating compliance. | No Exception |
| **TSC ref # CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.** | | |
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC6.8.1** The Organization deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. | Reviewed anti-malware policies and system documentation showing automated signature updates, alerting mechanisms, and reporting functionality.<br>Interviewed the Head of IT and Co-Founder and confirmed that anti-malware software is deployed across all relevant endpoints and routinely monitored.<br>The organization is using XProtect for Apple devices and also relies on compliance tool real-time detection. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC6.8.2** The Organization has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Reviewed SDLC documentation outlining structured processes for system development and changes, including requirements gathering, testing, approvals, and controlled deployment processes for production changes.<br>Interviewed the Head of IT and Co-Founder and confirmed that the SDLC is actively followed for enhancements and new system implementations, including emergency change handling.<br>Observed evidence of change records with testing artifacts and approval documentation supporting compliance with the SDLC methodology.<br>Reviewed GitHub and KanBan for project management of the active and completed requirements.<br>Daily Standup meetings are held for the review of the ongoing developments.<br>GitHub Advanced Security is used; Linear is used for software developments.<br>Development evidence reviewed for FRA-7079, 6938, & 6922. | No Exception |
| **TSC ref # CC6.8.3** The Organization has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Reviewed Fragment's vulnerability management and patching procedures showing scheduled updates and remediation based on risk.<br>Interviewed the Head of IT and Co-Founder and confirmed timely patching aligned with industry best practices and SLAs.<br>Observed patch deployment logs and reports confirming recent updates applied across in-scope systems.<br>AWS CloudTrail is enabled by the organization and integrated into the compliance platform.<br>GuardDuty alerts are integrated with Slack.<br>GitHub is used for vulnerability management, with Dependabot integrated for any CVEs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.7 System Operations

| TSC ref # CC7.1 - To meet its objectives, the entity user detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC7.1.1** The Organization requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Reviewed change management procedures requiring change requests, impact assessments, testing, approval, and implementation tracking.<br>Interviewed the Head of IT and Co-Founder and confirmed consistent enforcement of the change review and approval process.<br>There were no activities or changes on the infrastructure within the observation period. Although, changes related to the core software were observed and found satisfactory. | No Exception |
| **TSC ref # CC7.1.2** The Organization has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. | Observed that system configurations are defined and managed through Infrastructure-as-Code and deployed via automated CI/CD pipelines, ensuring consistency across all environments and AWS regions. Observed that AWS Control Tower and AWS Organizations provide centralized governance and account-level standardization. Configuration changes are controlled through GitHub pull requests requiring peer review and automated validation before deployment to production.<br>Interviewed the Head of IT who confirmed that all infrastructure and application configurations are deployed through standardized CI pipelines and that manual configuration changes in production environments are restricted. They further confirmed that Seed CI system enforces consistent environment provisioning and deployment controls.<br>Based on the procedures performed, configuration management practices are operating effectively and ensure consistent deployment of system configurations across the environment. No exceptions were noted. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.1.3** The Organization's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Reviewed Fragment's Risk Assessment documentation covering environmental, regulatory, and technological changes that could affect security commitments and objectives. Evidence included annual risk assessment reports and updates to controls based on identified risk.<br><br>Interviews with the Head of IT and Co-Founder confirmed that leadership incorporates fraud considerations into the annual risk assessment process and evaluates the likelihood and impact of fraud-related risks.<br><br>Observed documented results of the most recent annual risk assessment, including action plans for identified risks and review acknowledgment from senior management.<br><br>Reviewed the Risk snapshot on Vanta dated 09-Feb-2026, with a total of 10 Risks identified. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.1.4** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |
| **TSC ref # CC7.1.5** The Organization's formal policies outline the requirements for the following functions related to IT / Engineering:<br>▪ vulnerability management;<br>▪ system monitoring. | Reviewed policies outlining requirements for vulnerability scanning, remediation, system monitoring, event handling, and alerting.<br><br>Interviewed the Head of IT and Co-Founder and confirmed continuous monitoring practices and review of detection alerts via AWS GuardDuty.<br><br>Observed system monitoring alerts and logging dashboards demonstrating continuous visibility into system and network activity. Elastic logs go into PagerDuty.<br><br>The incident management platform Incident.io is used for incident tracking. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC7.2.1** An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Reviewed system and infrastructure performance monitoring procedures and alerts triggered by predefined threshold breaches.<br>Interviewed the Head of IT and Co-Founder and confirmed active monitoring of infrastructure health and automated alerting workflows.<br>Observed monitoring dashboards showing resource metrics and recent incident alerts routed to responsible personnel. | No Exception |
| **TSC ref # CC7.2.2** The Organization uses an intrusion detection system to provide continuous monitoring of the Organization's network and early detection of potential security breaches. | Reviewed AWS IDS configuration documentation showing continuous monitoring and alerting capabilities.<br>Interviewed the Head of IT and Co-Founder and confirmed security operations review alerts and perform incident response actions.<br>Observed AWS GuardDuty dashboard screens and historical alert logs demonstrating active monitoring.<br>The notifications and alerts on IDS are instantly taken up by the Engineering team. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.2.3** The Organization utilizes a log management tool to identify events that may have a potential impact on the Organization's ability to achieve its security objectives. | Reviewed log management configuration documentation and event monitoring procedures outlining how system activity is monitored and analyzed for security-related events.<br>Interviewed the Head of IT and Co-Founder and confirmed that logs are reviewed regularly and alerts are escalated per defined thresholds.<br>AWS Native Applications are implemented to observe any abnormal behaviors of the cloud infrastructure, and alerts are instantly reviewed by the DevOps teams.<br>AWS GuardDuty and AWS CloudWatch are integrated for security and observability alerts.<br>Observed screenshots/log samples demonstrating active event logging and timely alert generation for abnormal or unauthorized activities. | No Exception |
| **TSC ref # CC7.2.4** The Organization's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs. | Reviewed Fragment's Operational Security Policy; the penetration test is conducted annually.<br>Interviewed the Head of IT and Co-Founder and confirmed a penetration test was conducted by CL, dated 06-Mar-2026. Three Medium-level vulnerabilities were identified.<br>The organization presented the remediations of these vulnerabilities. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.2.5** The Organization has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Reviewed Fragment's vulnerability management and patching procedures showing scheduled updates and remediation based on risk.<br>Interviewed the Head of IT and Co-Founder and confirmed timely patching aligned with industry best practices and SLAs.<br>Observed patch deployment logs and reports confirming recent updates applied across in-scope systems.<br>AWS CloudTrail is enabled by the organization and integrated into the compliance platform.<br>GuardDuty alerts are integrated with Slack.<br>GitHub is used for vulnerability management, with Dependabot integrated for any CVEs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.2.6** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |
| **TSC ref # CC7.2.7** The Organization's formal policies outline the requirements for the following functions related to IT / Engineering:<br>▪ vulnerability management;<br>▪ system monitoring. | Reviewed policies outlining requirements for vulnerability scanning, remediation, system monitoring, event handling, and alerting.<br><br>Interviewed the Head of IT and Co-Founder and confirmed continuous monitoring practices and review of detection alerts via AWS GuardDuty.<br><br>Observed system monitoring alerts and logging dashboards demonstrating continuous visibility into system and network activity. Elastic logs go into PagerDuty.<br><br>The incident management platform Incident.io is used for incident tracking. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC7.3.1** The Organization's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Organization's security incident response policy and procedures. | Reviewed Fragment's incident response logs and ticketing records showing logging, investigation, resolution, and communication workflows, aligned with the incident response procedures.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that all security and privacy incidents are tracked through defined escalation channels and communicated to impacted parties when applicable.<br><br>Observed that operational and security alerts generated by CloudWatch and Elastic are routed to PagerDuty, which is integrated with Incidents.io to support incident lifecycle management, including tracking, escalation, investigation, resolution, and post-incident documentation. Management indicated that direct Elastic integration with Incidents.io is planned for future implementation.<br><br>Observed that security logs are retained for 13 months to support incident investigations, root cause analysis, and compliance requirements. | No Exception |
| **TSC ref # CC7.3.2** The Organization has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Reviewed incident response policies, incident reporting workflows, and communication protocols that define how personnel must report and respond to cybersecurity and privacy incidents.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that employees are informed of reporting channels and escalation expectations during onboarding and refresher training.<br><br>Observed access to incident response documentation on internal platforms (i.e., Slack).<br><br>Reviewed the one incident related to the service downtime.<br><br>The incident management platform Incident.io is used for incident tracking. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC7.4.1** The Organization's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Organization's security incident response policy and procedures. | Reviewed Fragment's incident response logs and ticketing records showing logging, investigation, resolution, and communication workflows, aligned with the incident response procedures.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that all security and privacy incidents are tracked through defined escalation channels and communicated to impacted parties when applicable.<br><br>Observed that operational and security alerts generated by CloudWatch and Elastic are routed to PagerDuty, which is integrated with Incidents.io to support incident lifecycle management, including tracking, escalation, investigation, resolution, and post-incident documentation. Management indicated that direct Elastic integration with Incidents.io is planned for future implementation.<br><br>Observed that security logs are retained for 13 months to support incident investigations, root cause analysis, and compliance requirements. | No Exception |
| **TSC ref # CC7.4.2** The Organization tests their incident response plan at least annually. | Reviewed Fragment's Incident Response Plan and documentation of incident response plan testing activities, including test scenarios, participant lists, and results summary reports. Examined records showing the scope, methodology, and outcomes of the annual testing exercise.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that incident response plan testing is conducted at least annually. Management described the testing approach, including tabletop exercises and simulated incident scenarios used to validate the effectiveness of response procedures.<br><br>Observed dated evidence of the most recent incident response tabletop exercise conducted on 14-May-2026. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.4.3** The Organization has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Reviewed incident response policies, incident reporting workflows, and communication protocols that define how personnel must report and respond to cybersecurity and privacy incidents.<br>Interviewed the Head of IT and Co-Founder and confirmed that employees are informed of reporting channels and escalation expectations during onboarding and refresher training.<br>Observed access to incident response documentation on internal platforms (i.e., Slack).<br>Reviewed the one incident related to the service downtime.<br>The incident management platform Incident.io is used for incident tracking. | No Exception |
| **TSC ref # CC7.4.4** The Organization has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Reviewed Fragment's vulnerability management and patching procedures showing scheduled updates and remediation based on risk.<br>Interviewed the Head of IT and Co-Founder and confirmed timely patching aligned with industry best practices and SLAs.<br>Observed patch deployment logs and reports confirming recent updates applied across in-scope systems.<br>AWS CloudTrail is enabled by the organization and integrated into the compliance platform.<br>GuardDuty alerts are integrated with Slack.<br>GitHub is used for vulnerability management, with Dependabot integrated for any CVEs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.4.5** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC7.5.1** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.5.2** The Organization's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Organization's security incident response policy and procedures. | Reviewed Fragment's incident response logs and ticketing records showing logging, investigation, resolution, and communication workflows, aligned with the incident response procedures.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that all security and privacy incidents are tracked through defined escalation channels and communicated to impacted parties when applicable.<br><br>Observed that operational and security alerts generated by CloudWatch and Elastic are routed to PagerDuty, which is integrated with Incidents.io to support incident lifecycle management, including tracking, escalation, investigation, resolution, and post-incident documentation. Management indicated that direct Elastic integration with Incidents.io is planned for future implementation.<br><br>Observed that security logs are retained for 13 months to support incident investigations, root cause analysis, and compliance requirements. | No Exception |
| **TSC ref # CC7.5.3** The Organization tests their incident response plan at least annually. | Reviewed Fragment's Incident Response Plan, documentation of incident response plan testing activities, including test scenarios, participant lists, and results summary reports. Examined records showing the scope, methodology, and outcomes of the annual testing exercise.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that incident response plan testing is conducted at least annually. Management described the testing approach, including tabletop exercises and simulated incident scenarios used to validate the effectiveness of response procedures.<br><br>Observed dated evidence of the most recent incident response tabletop exercise conducted on 14-May-2026. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC7.5.4** The Organization has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Reviewed incident response policies, incident reporting workflows, and communication protocols that define how personnel must report and respond to cybersecurity and privacy incidents.<br>Interviewed the Head of IT and Co-Founder and confirmed that employees are informed of reporting channels and escalation expectations during onboarding and refresher training.<br>Observed access to incident response documentation on internal platforms (i.e., Slack).<br>Reviewed the one incident related to the service downtime.<br>The incident management platform Incident.io is used for incident tracking. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.8 Change Management

| TSC ref # CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC8.1.1** The Organization requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Reviewed change management procedures requiring change requests, impact assessments, testing, approval, and implementation tracking.<br>Interviewed the Head of IT and Co-Founder and confirmed consistent enforcement of the change review and approval process.<br>There were no activities or changes on the infrastructure within the observation period. Although, changes related to the core software were observed and found satisfactory. | No Exception |
| **TSC ref # CC8.1.2** The Organization has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Reviewed SDLC documentation outlining structured processes for system development and changes, including requirements gathering, testing, approvals, and controlled deployment processes for production changes.<br>Interviewed the Head of IT and Co-Founder and confirmed that the SDLC is actively followed for enhancements and new system implementations, including emergency change handling.<br>Observed evidence of change records with testing artifacts and approval documentation supporting compliance with the SDLC methodology.<br>Reviewed GitHub and KanBan for project management of the active and completed requirements. Daily Standup meetings are held for the review of the ongoing developments.<br>GitHub Advanced Security is used; Linear is used for software developments.<br>Development evidence reviewed for FRA-7079, 6938, & 6922. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC8.1.3** The Organization's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. | Reviewed documented hardening guidelines derived from industry standards with annual review evidence.<br>Interviewed the Head of IT and Co-Founder and confirmed that infrastructure is deployed and maintained per defined security standards.<br>Fragment's network and system hardening is enforced through AWS Organizations and Control Tower, applying consistent security guardrails across all environments based on AWS industry best practices. Infrastructure is managed entirely as Infrastructure as Code (IaC), ensuring all system configurations are documented, version-controlled, and consistently applied across all environments. AWS CloudTrail and GuardDuty provide continuous monitoring against hardening standards, with alerts integrated into Slack. | No Exception |
| **TSC ref # CC8.1.4** The Organization's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs. | Reviewed Fragment's Operational Security Policy; the penetration test is conducted annually.<br>Interviewed the Head of IT and Co-Founder and confirmed a penetration test was conducted by CL, dated 06-Mar-2026. Three Medium-level vulnerabilities were identified.<br>The organization presented the remediations of these vulnerabilities. | No Exception |
| **TSC ref # CC8.1.5** The Organization restricts access to migrate changes to production to authorized personnel. | Reviewed change management procedures requiring authorization, peer validation, and approvals before deployment to production.<br>Interviewed the Head of IT and Co-Founder and confirmed that only specified personnel can deploy production changes.<br>Observed change deployment logs showing restricted execution of migration activities.<br>Access is limited to the Engineering team's specific admin only. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC8.1.6** The Organization has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Reviewed Fragment's vulnerability management and patching procedures showing scheduled updates and remediation based on risk.<br><br>Interviewed the Head of IT and Co-Founder and confirmed timely patching aligned with industry best practices and SLAs.<br><br>Observed patch deployment logs and reports confirming recent updates applied across in-scope systems.<br><br>AWS CloudTrail is enabled by the organization and integrated into the compliance platform.<br><br>GuardDuty alerts are integrated with Slack.<br><br>GitHub is used for vulnerability management, with Dependabot integrated for any CVEs. | No Exception |
| **TSC ref # CC8.1.7** Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Reviewed the organization's vulnerability management processes and configurations within GitHub. Observed that GitHub Advanced Security and Dependabot are implemented to continuously identify vulnerabilities and Common Vulnerabilities and Exposures (CVEs) affecting application dependencies and code repositories. Reviewed evidence demonstrating that vulnerability findings are generated automatically and tracked through GitHub workflows until remediation.<br><br>Reviewed the organization's AWS environment and observed the use of AWS Organizations, AWS Control Tower, AWS CloudTrail, and AWS GuardDuty. Confirmed that GuardDuty security findings and alerts are integrated with Slack to facilitate timely review and response by responsible personnel.<br><br>Interviewed the Head of IT and Co-Founder, who confirmed that the organization utilizes automated vulnerability monitoring through GitHub Advanced Security and Dependabot rather than periodic manual host-based scans. They further confirmed that identified critical and high-risk vulnerabilities are assigned, tracked, and remediated through the organization's established issue management processes.<br><br>Observed vulnerability reports, remediation tickets, and security alert records demonstrating that identified vulnerabilities are monitored and remediated in a timely manner. Reviewed logging configurations and confirmed that security logs are retained for a period of 13 months to support security monitoring, investigations, and compliance requirements. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

### 4.1.9 Risk Mitigation

| TSC ref # CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref CC 9.1.1** The Organization has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | Reviewed the organization's Business Continuity and Disaster Recovery (BC/DR) Plan, including defined recovery responsibilities, communication procedures, recovery time objectives, and documented protocols for business service restoration. Also reviewed evidence of periodic BC/DR testing and resulting corrective action plans.<br><br>Interviewed the Head of IT and Co-Founder and confirmed that BC/DR exercises are conducted at least annually, and lessons learned from tests are used to improve resiliency.<br><br>Observed evidence of recent BC/DR test results dated 14-May-2026, including test dates, scope, management approvals, and documented follow-up activities to address identified gaps.<br><br>Observed that incident notifications and operational alerts are routed through PagerDuty and communicated through established escalation workflows like Slack, enabling responsibilities to be transferred to alternate personnel when necessary. Incidents.io is utilized to coordinate response activities and maintain visibility into ongoing incidents. | No Exception |
| **TSC ref # CC 9.1.2** The Organization maintains cybersecurity insurance to mitigate the financial impact of business disruptions. | Interviewed the Head of IT and Co-Founder and noted that Fragment Concepts does hold cyber cybersecurity insurance to reduce the financial impact of business disruptions.<br><br>The organization is enrolled in Embroker's Startup Package Plus bundled insurance program, which expires on 03-Jul-2027. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| | | |
|---|---|---|
| **TSC ref # CC 9.1.3** The Organization's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Reviewed Fragment's Risk Assessment documentation covering environmental, regulatory, and technological changes that could affect security commitments and objectives. Evidence included annual risk assessment reports and updates to controls based on identified risk.<br>Interviews with the Head of IT and Co-Founder confirmed that leadership incorporates fraud considerations into the annual risk assessment process and evaluates the likelihood and impact of fraud-related risks.<br>Observed documented results of the most recent annual risk assessment, including action plans for identified risks and review acknowledgment from senior management.<br>Reviewed the Risk snapshot on Vanta dated 09-Feb-2026, with a total of 10 Risks identified. | No Exception |
| **TSC ref # CC 9.1.4** The Organization has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Reviewed the organization's risk management policy and risk register, which define procedures for risk assessment, likelihood and impact scoring, and implementation of mitigation actions.<br>Interviewed the Head of IT and Co-Founder and confirmed ownership of risk management activities within management, including periodic review of risk posture and escalation of high-severity risks.<br>Observed examples of tracked risks with assigned owners, statuses, and planned mitigation timelines within the risk management system.<br>Reviewed the recent Risk snapshot dated 09-Feb-2026 on the compliance platform.<br>There are 10 Risks identified in the risk register currently available on the compliance platform. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

| TSC ref # CC9.2 - The entity assesses and manages risk associated with vendors and business partners. | | |
|---|---|---|
| **Control Description** | **Test of Controls** | **Results** |
| **TSC ref # CC 9.2.1** The Organization has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Reviewed executed vendor agreements including security, confidentiality, and data protection clauses governing the handling of company or customer information.<br>Interviews with the Head of IT and Co-Founder confirmed formal due diligence, and contracting is required before granting access to systems or data.<br>Observed monitored vendor contract records stored within the compliance platform for listed vendors (e.g., Vanta, GCP, Linear, Slack, and Certn). | No Exception |
| **TSC ref # CC9.2.2** The Organization has a vendor management program in place. Components of this program include:<br>▪ critical third-party vendor inventory;<br>▪ vendor's security and privacy requirements; and<br>▪ review of critical third-party vendors at least annually. | Reviewed the vendor management policy and third-party inventory identifying critical suppliers, along with contracts defining security and confidentiality requirements.<br>Interviews with the Head of IT and Co-Founder verified that vendor oversight responsibilities include periodic review of vendor performance and security posture, with results reported to management.<br>Observed evidence of an annual vendor review process including assessment of security documentation, compliance confirmations, and contractual obligations.<br>Observed the security reviews completed for all the critical, high, medium and low vendors by the Head of IT and relevant POCs. | No Exception |



Joseph Weindorfer, CPA | Email: joseph@consilium-labs.com

# Audit trail

## Details

| | |
|---|---|
| FILE NAME | Fragment - Form 046 SOC2 Audit Report VANTA Controls v3.1 - 6/24/26, 3:14 AM.pdf |
| STATUS | Signed |
| STATUS TIMESTAMP | 2026/06/24<br>20:19:21 UTC |

## Activity

| | | |
|---|---|---|
| SENT | zea@consilium-labs.com **sent** a signature request to:<br>• Joseph Wiendorfer (joseph@consilium-labs.com) | 2026/06/23<br>19:15:01 UTC |
| SIGNED | **Signed** by Joseph Wiendorfer (joseph@consilium-labs.com) | 2026/06/24<br>20:19:21 UTC |
| COMPLETED | This document has been signed by all signers and is **complete** | 2026/06/24<br>20:19:21 UTC |

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.