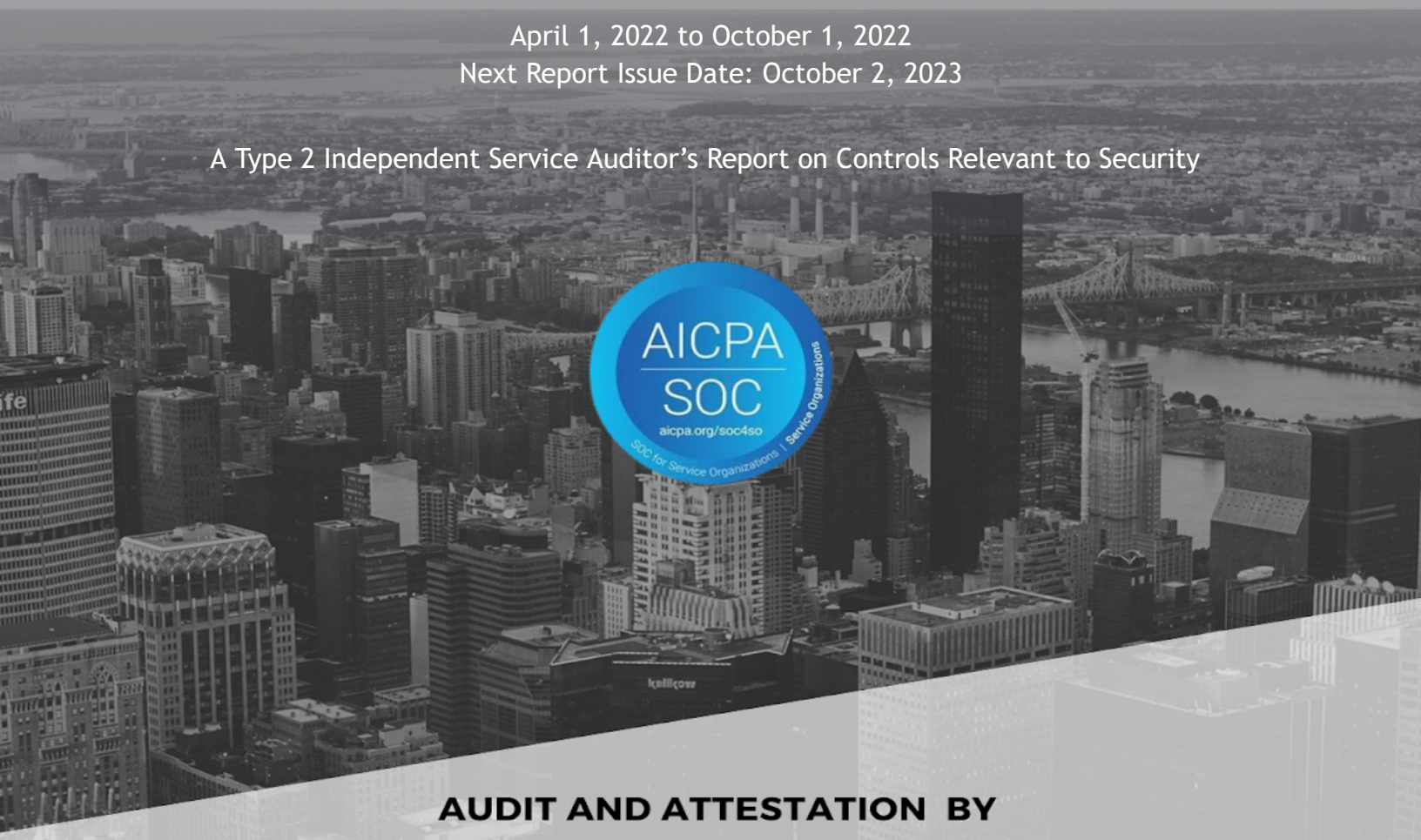
SOC 2 Type 2 Report

Mainstem Inc

April 1, 2022 to October 1, 2022

Next Report Issue Date: October 2, 2023

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security



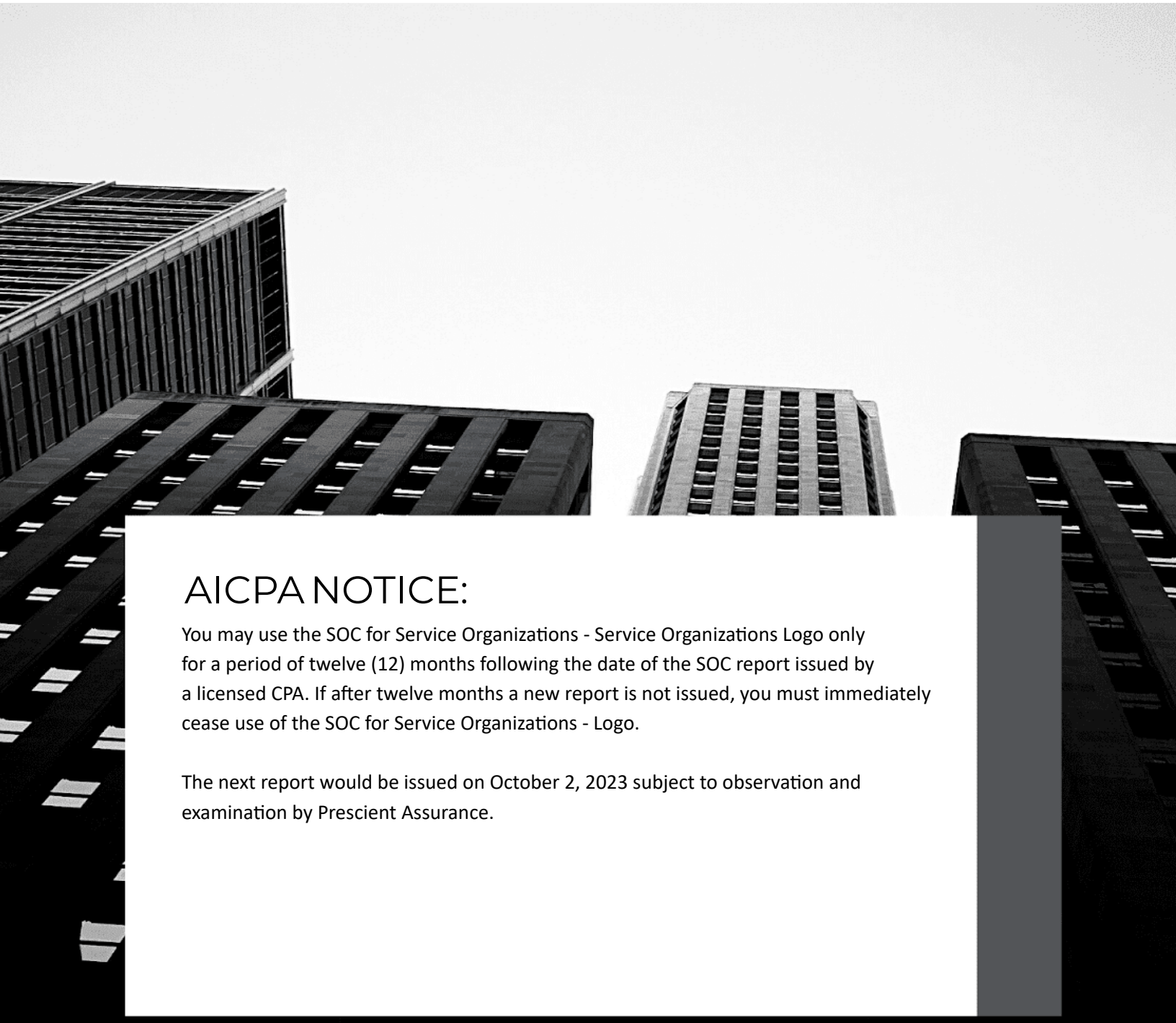
AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319



AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

The next report would be issued on October 2, 2023 subject to observation and examination by Prescient Assurance.

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Mainstem Inc's system throughout the period April 1, 2022, to October 1, 2022, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Mainstem Inc's system that may be useful when assessing the risks arising from interactions with Mainstem Inc's system, particularly information about system controls that Mainstem Inc has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

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

a. The description presents Mainstem Inc's system that was designed and implemented throughout the period April 1, 2022, to October 1, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 1, 2022, to October 1, 2022, to provide reasonable assurance that Mainstem Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Mainstem Inc's controls during that period.
c. The controls stated in the description operated effectively throughout the period April 1, 2022, to October 1, 2022, to provide reasonable assurance that Mainstem Inc's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Mainstem Inc's controls operated effectively throughout the period.

DocuSigned by:
Garrett Hampton
1BF124FC6F3F4D1...

Garrett Hampton
CTO
Mainstem Inc

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Mainstem Inc

Scope

We have examined Mainstem Inc's ("Mainstem Inc") accompanying description of its Mainstem system found in Section 3, titled Mainstem Inc System Description throughout the period April 1, 2022, to October 1, 2022, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022, to October 1, 2022, to provide reasonable assurance that Mainstem Inc's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Mainstem Inc uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mainstem Inc, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Mainstem Inc's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Mainstem Inc's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Mainstem Inc, to achieve Mainstem Inc's service commitments and system requirements based on the applicable trust services criteria. The description presents Mainstem Inc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mainstem Inc's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Mainstem Inc is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Mainstem Inc's service commitments and system requirements were achieved. In Section 1, Mainstem Inc has provided the accompanying assertion titled "Management's Assertion of Mainstem Inc" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Mainstem Inc is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. 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.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. 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.
5. 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.
6. Evaluating the overall presentation of the description.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design 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 the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects:

a. The description presents the Mainstem Inc's system that was designed and implemented throughout the period April 1, 2022, to October 1, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 1, 2022, to October 1, 2022, to provide reasonable assurance that Mainstem Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Mainstem Inc's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period April 1, 2022, to October 1, 2022, to provide reasonable assurance that Mainstem Inc's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Mainstem Inc's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Mainstem Inc, user entities of Mainstem Inc's system during some or all of the period April 1, 2022 to October 1, 2022, business partners of Mainstem Inc subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. 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.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
May 5, 2023

SECTION 3

System Description

DC 1: Company Overview and Types of Products and Services Provided

Mainstem, inc. is a technology company headquartered in Seattle, WA that provides b2b supply chain tools to enable companies to buy and sell supplies and streamline their supply chain.

Mainstem offers an online platform that provides businesses with a B2B supply chain toolkit.

The mainstem platform focuses on location, user management, products, services, vendors, purchasing, payments, and shipments. The platform relies on integrations, API, and homogenized data.

DC 2: The Principal Service Commitments and System Requirements

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

Mainstem's commitments to users are communicated through service level agreements (SLAs) or master service agreements (MSAs), online privacy policy.

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

DC 3: The Components of the System Used to Provide the Services

The System is comprised of the following components:

- 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.

3.1 Primary Infrastructure

MainStem, 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).

Primary Infrastructure		
Hardware	Type	Purpose
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
Azure Platform	Azure	Managed cloud platform where services are hosted
Azure Virtual Machine	Azure	Virtual machine service for web hosting and backend service offerings

Primary Infrastructure		
Hardware	Type	Purpose
Azure Kubernetes	Azure	Container orchestration for deployment, scaling, and management
Azure Database	Azure	Transactional database with backups and redundancy

3.2 Primary Software

MainStem, Inc. is responsible for managing the development and operation of the MainStem system including infrastructure components such as servers, databases, and storage systems. The in-scope MainStem, 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 MainStem, Inc. platform
Azure SDK	N/A	The SDK is used to communicate with Microsoft azure web services

3.3 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.

MainStem, Inc. has 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 - Alen Nguyen
CTO - Garrett Hampton

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.

3.4 Data

Data as defined by MainStem, 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 MainStem, Inc.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for MainStem, Inc.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by MainStem, Inc.. MainStem, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer

Category	Description	Examples
Company data	Information collected and used by MainStem, Inc. to operate the business. MainStem, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • 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 employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, MainStem, 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.

3.5 Processes 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

Physical security

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

Logical access

MainStem, 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 reportable user provisioning and deprovisioning processes.

Access to these systems are 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.

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 MainStem, Inc.'s policies, completing security training. These steps must be completed within 1 day of hire.

When an employee is terminated, management is responsible for deprovisioning access to all in scope systems within 1 day of that employee's termination.

Computer operations - backups

Customer data is backed up and monitored by the IT team, CTO for completion and exceptions. If there is an exception, IT team, CTO 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 Microsoft Azure and AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer operations - availability

MainStem, 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.

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

MainStem, 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.

Change management

MainStem, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

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

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

Data communications

MainStem, 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 MainStem, 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.

Mainstem inc uses an automated monitoring service to perform quarterly 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.

Boundaries of the system

The boundaries of the MainStem 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 MainStem.

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

DC 4: Disclosures About Identified Security Incidents

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

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

5.1 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 MainStem, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of MainStem, Inc.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. 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.

5.2 Commitment to competence

MainStem, 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.

5.3 Management's philosophy and operating style

The MainStem, 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 MainStem, 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 MainStem, 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.

5.4 Organizational structure and assignment of authority and responsibility

MainStem, 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.

MainStem, Inc.'s assignment of authority and responsibility activities includes 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.

5.5 HR policies and practices

MainStem, 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. MainStem, Inc.'s human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement 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.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6 Risk assessment process

MainStem, Inc. risk assessment process identifies and manages risks that could potentially affect MainStem, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, MainStem, 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 MainStem, Inc. product development process so they can be dealt with predictably and iteratively.

5.7 Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of MainStem, Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. MainStem, 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, MainStem, Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information and communication systems

Information and communication are an integral component of MainStem, 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.

MainStem, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. MainStem, 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, MainStem, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.9 Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. MainStem, 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.

5.9.1 On-going Monitoring

MainStem, 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 MainStem, 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 MainStem, Inc.'s personnel.

Reporting 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.

DC 6: Complementary User Entity Controls

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

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.

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

DC 7: Complementary Subservice Organization Controls

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

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services. The Cloud Hosting Services provided by Azure support the physical infrastructure of the entities services.

MainStem, 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 MainStem, Inc.'s services to be solely achieved by MainStem, Inc. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of MainStem, Inc.

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

Azure

Category	Criteria	Control
Security	CC 6.4	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
Security	CC 6.4	Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
Security	CC 6.4	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
Security	CC 6.4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
Security	CC 6.4	The datacenter facility is monitored 24x7 by security personnel.

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 camera (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.

MainStem, 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, MainStem, 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)
- 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

DC 8: Disclosures of out of scope Trust Services Criteria

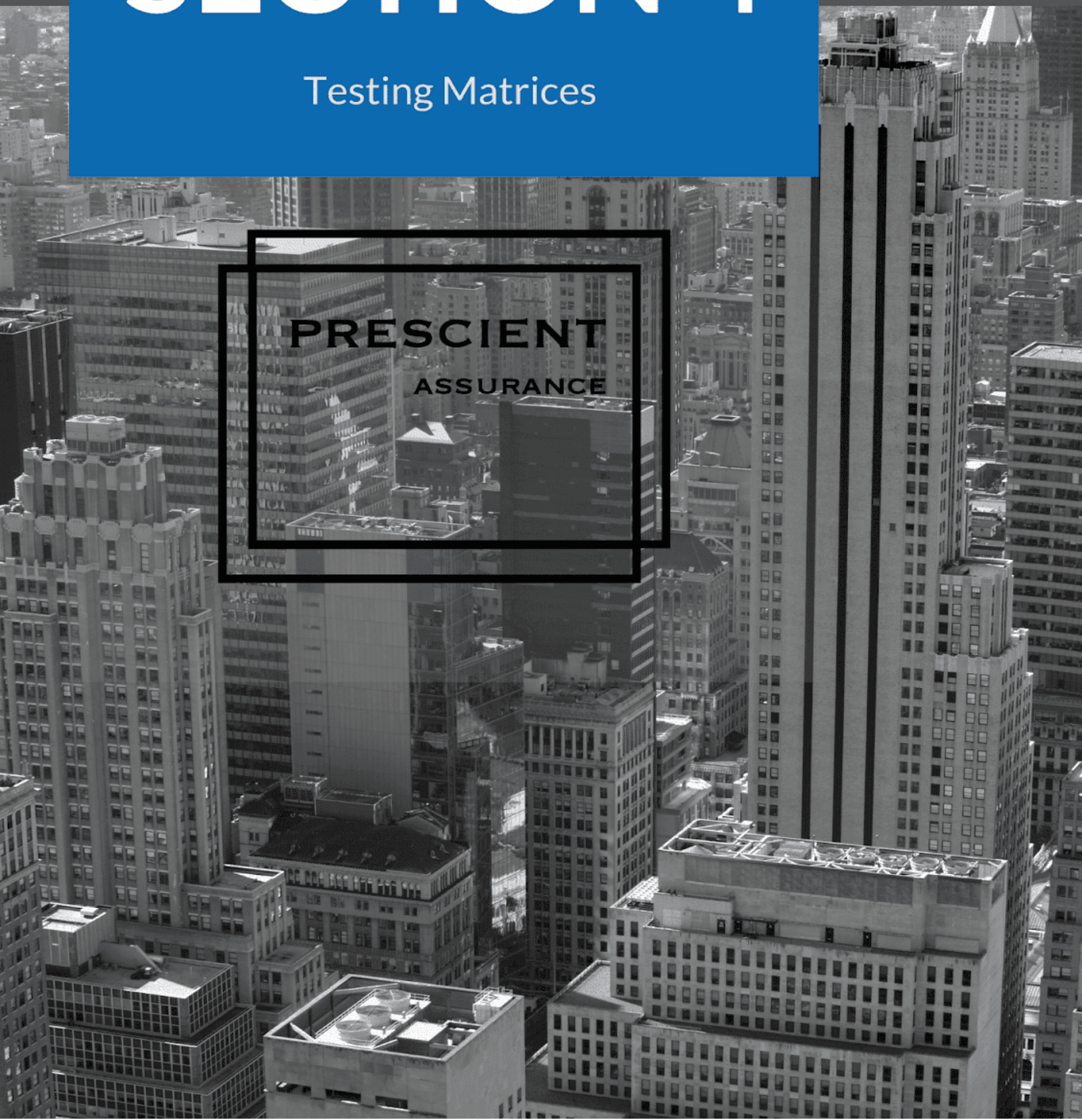
All Security criteria were applicable to the MainStem, Inc.'s Mainstem system.

DC 9: Disclosures of Significant Changes in last 1 year

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

SECTION 4

Testing Matrices



Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Mainstem provided by Mainstem Inc. The scope of the testing was restricted to Mainstem, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period April 1, 2022, to October 1, 2022.

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: • Examination/Inspection of source documentation and authorizations to verify transactions processed. • Examination/Inspection of documents or records for evidence of performance, such as existence of initials or signatures. • Examination/Inspection of systems documentation, configurations, and settings; and • Examination/Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.

Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	**At least 40**
Manual control, daily (Note 1)	At least 25	**At least 40**
Manual control, weekly	At least 5	**At least 10**
Manual control, monthly	At least 3	**At least 4**

Manual control, quarterly	At least 2	**At least 2**
Manual control, annually	Test annually	**Test annually**
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	**Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25**
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	**Follow guidance above for manual and automated aspects of IT general controls**

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices.

Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity.

Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	Standard Description	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Observed through Vanta that Mainstem Inc uses Checkr to perform background checks on new employees. Observed the background check reports for a sample of employees which show the clear status for the employees, to determine that the company conducts background checks for all new employees. Inspected the Human Resource Security Policy which states that background verification checks on personnel are to be carried out in accordance with relevant laws and regulations, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks, to determine that the company is required to conduct background checks for all new employees.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected a Contractor Agreement template which states that the consultant agrees to comply with all rules and procedures for accessing and using the company, premises and equipment, including those related to safety and security, to determine that the contractor agrees to provide services while acting in line with the company's policies. Inspected the Code of Conduct which states that its terms apply to all contractor staff and that they are required to abide by it in all daily affairs including professional functions and events, to determine that the company requires contractor agreements to include a Code of Conduct or reference to it. Disclosure: There were no contractors hired during the observation period.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company 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	Observed the data exported through Vanta which shows that all relevant employees have accepted the Code of Conduct and Human Resource Security Policy to determine that the Code of Conduct and the penalties for violating its terms are acknowledged by employees at the time of hire. Inspected the Code of Conduct which states that	No exceptions noted.

		accordance with a disciplinary policy.	its terms apply to all employees, to determine that the company requires employees to acknowledge the Code of Conduct at the time of hire. Inspected the Human Resource Security Policy which states that employees who violate Mainstem Inc's information security policies shall be subject to Mainstem Inc's progressive disciplinary process, up to and including termination of employment or contract, to determine that the company has a disciplinary process in place for violations of the Code of Conduct by employees.	
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected a Consulting Agreement template which includes a Proprietary Information clause which states that the consultant will hold in confidence and not disclose or, except in performing the services, use any proprietary information, to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement. Inspected the Human Resource Security Policy which states that third parties with access to company or customer information shall sign an appropriate non-disclosure or confidentiality agreement and that contractual agreements shall state responsibilities for information security, to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected a signed Employee Inventions Assignment, Confidentiality, and Non-Competition Agreement, which includes clauses related to confidential information, to determine that employees sign a confidentiality agreement at the time of hire. Inspected the Human Resource Security Policy which states that employees with access to company or customer information shall sign an appropriate non-disclosure or confidentiality agreement to determine that the company requires employees to sign a confidentiality agreement at the time of onboarding.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates	The company's board of directors or a relevant subcommittee is briefed by	Inspected the minutes of a meeting of the board of directors dated November 7, 2022, which includes discussions on revenue performance, customer	No exceptions noted.

	independence from management and exercises oversight of the development and performance of internal control.	senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	spending, corporate partnerships, strategic model completion, and a data launch, to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk.	
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected Mainstem Inc Board Charter which states that the Board of Directors is responsible for reviewing and approving the strategic direction and major decisions of the organization to make sure it is in line with the shareholders' best interests, to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company'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.	Inspected the Linkedin profiles of the Chairman/CEO and other board members, which show their qualifications, skills, and experience, to determine that the company's board members have sufficient expertise to oversee the management's ability to design, implement and operate information security controls.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the minutes of a meeting of the board of directors dated November 7, 2022, which includes discussions on revenue performance, customer spending, corporate partnerships, strategic model completion, and a data launch, to determine that the company's board of directors meets at least annually and maintains formal meeting minutes. Inspected the LinkedIn profile of Matthew Smith, who is an independent member of the board, to determine that the board includes directors that are independent of the company.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected Mainstem Inc Board Charter which states that the Board of Directors is responsible for reviewing and approving the strategic direction and major decisions of the organization to make sure it is in line with the shareholders' best interests, to determine that the company's board of directors has a documented charter that	No exceptions noted.

	the pursuit of objectives.		outlines its oversight responsibilities for internal control.	
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for oversight of IS controls. Inspected the Information Security Roles and Responsibilities Policy's section titled "Audience" which states that the Board of Directors, Executive Leadership, and CTO are responsible for the oversight over cyber-risk and internal control, execution of the information security risk management program and risk treatments, and the design, development, implementation, operation, maintenance and monitoring of IT security controls, to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart of the company which identifies the company CEO as the head of the organization, and that the Head of Finance and HR, CTO, CRO, and Vice President of Operations report to the CEO, to determine that the company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	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.	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for information security. Inspected the Information Security Roles and Responsibilities Policy section titled "Audience" which states that the employees and contractors of the company are responsible for acting at all times in a manner that does not place at risk the health and safety of themselves, other people in the workplace, and the information and resources they have use of, helping to identify areas where risk management practices should be adopted, taking all practical steps to minimize the company's exposure to contractual and regulatory liability,	No exceptions noted.

			adhering to company policies and standards of conduct and reporting incidents and observed anomalies or weaknesses to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Observed through Vanta that Mainstem Inc uses Checkr to perform background checks on new employees. Observed the background check reports for a sample of employees which show the clear status for the employees, to determine that the company conducts background checks for all new employees. Inspected the Human Resource Security Policy which states that background verification checks on personnel are to be carried out in accordance with relevant laws and regulations, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks, to determine that the company is required to conduct background checks for all new employees.	No exceptions noted.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	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.	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for information security. Inspected the Information Security Roles and Responsibilities Policy section titled "Audience" which states that the employees and contractors of the company are responsible for acting at all times in a manner that does not place at risk the health and safety of themselves, other people in the workplace, and the information and resources they have use of, helping to identify areas where risk management practices should be adopted, taking all practical steps to minimize the company's exposure to contractual and regulatory liability, adhering to company policies and standards of conduct and reporting incidents and observed anomalies or weaknesses to determine that roles and responsibilities for the design, development,	No exceptions noted.

			implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Observed through Vanta that all relevant employees have completed the general security awareness training, to determine that security awareness training is implemented at the company. Inspected the Human Resource Security Policy which states that all employees and third parties with administrative or privileged technical access to the company's production systems and networks shall complete security awareness training at the time of hire and annually thereafter, to determine that the company requires all employees to complete security awareness training at the time of hire and annually thereafter.	No exceptions noted.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company 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.	Observed the data exported through Vanta which shows that all relevant employees have accepted the Code of Conduct and Human Resource Security Policy to determine that the Code of Conduct and the penalties for violating its terms are acknowledged by employees at the time of hire. Inspected the Code of Conduct which states that its terms apply to all employees, to determine that the company requires employees to acknowledge the Code of Conduct at the time of hire. Inspected the Human Resource Security Policy which states that employees who violate Mainstem Inc's information security policies shall be subject to Mainstem Inc's progressive disciplinary process, up to and including termination of employment or contract, to determine that the company has a disciplinary process in place for violations of the Code of Conduct by employees.	No exceptions noted.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for information security. Inspected the Information Security Roles and Responsibilities Policy section titled "Audience" which states that the employees and contractors of	No exceptions noted.

		and/or the Roles and Responsibilities policy.	the company are responsible for acting at all times in a manner that does not place at risk the health and safety of themselves, other people in the workplace, and the information and resources they have use of, helping to identify areas where risk management practices should be adopted, taking all practical steps to minimize the company's exposure to contractual and regulatory liability, adhering to company policies and standards of conduct and reporting incidents and observed anomalies or weaknesses to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company 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.	Observed that the company uses Vanta for performing internal self-assessments on a continuous basis. Inspected the Risk Management Policy section titled "Practical Application of Risk Management" which states that the company shall review and update its risk assessment and perform an internal audit of the information security management system at least annually, and that security risks shall be evaluated at various stages of the software design and development lifecycle as needed, to determine that the company is required to perform annual control self-assessments.	No exceptions noted.
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Observed the data exported through Vanta which shows that Office, Jira, Azure, Microsoft Endpoint Manager, GitHub, AWS, Checkr, Gusto, and Confluence infrastructures are linked to Vanta, to determine that activity on these applications is tracked on Vanta. Observed through Vanta that all linked AWS accounts have CloudTrial enabled, Azure security groups have flow logs enabled, AWS S3 server logs are enabled with access allowed only to authorized users, AWS CloudWatch Log Groups retain logs for at least 365 days, and VPC flow logs are enabled, to determine that logging is performed at the company on a regular basis.	No exceptions noted.

			Inspected the Operations Security Policy's section titled "Logging & Monitoring" which states that production infrastructure is to be configured to produce detailed event logs appropriate to the function served by the system or device, including user activity, exceptions, faults, and information security events, to determine that the company is required to utilize log management.	
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, observed screenshots which show that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that critical and high vulnerabilities are tracked to remediation. Inspected the Operations Security Policy section titled "Technical Vulnerability Management" which states that external vulnerability scans are required to be run on the production environment at least quarterly, vulnerabilities should be evaluated, and appropriate measures should be taken to address the associated risks, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems, with critical and high vulnerabilities tracked to remediation.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Observed through Vanta that all relevant employees have accepted the Incident Response Plan to determine that the plan is communicated to authorized users. Inspected the Incident Response Plan which provides guidance for reporting, categorizing, escalating, and documenting security incidents, the steps to be followed in responding to an incident, and the roles and responsibilities of response team members, to determine that security and privacy incident response policies have been documented by the management.	No exceptions noted.

CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for oversight of IS controls. Inspected the Information Security Roles and Responsibilities Policy's section titled "Audience" which states that the Board of Directors, Executive Leadership, and CTO are responsible for the oversight over cyber-risk and internal control, execution of the information security risk management program and risk treatments, and the design, development, implementation, operation, maintenance and monitoring of IT security controls, to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	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.	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for information security. Inspected the Information Security Roles and Responsibilities Policy section titled "Audience" which states that the employees and contractors of the company are responsible for acting at all times in a manner that does not place at risk the health and safety of themselves, other people in the workplace, and the information and resources they have use of, helping to identify areas where risk management practices should be adopted, taking all practical steps to minimize the company's exposure to contractual and regulatory liability, adhering to company policies and standards of conduct and reporting incidents and observed anomalies or weaknesses to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates	The company requires employees to complete security awareness training	Observed through Vanta that all relevant employees have completed the general security awareness training, to determine that security	No exceptions noted.

	information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	within thirty days of hire and at least annually thereafter.	awareness training is implemented at the company. Inspected the Human Resource Security Policy which states that all employees and third parties with administrative or privileged technical access to the company's production systems and networks shall complete security awareness training at the time of hire and annually thereafter, to determine that the company requires all employees to complete security awareness training at the time of hire and annually thereafter.	
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy section titled "Management Responsibilities" which states that management shall be responsible for ensuring that the information security policies and procedures are reviewed annually and made accessible to all employees and contractors. Observed through Vanta that the Access Control Policy, Asset Management Policy, Cryptography Policy, and other policies were approved on August 07, 2022, and August 08, 2022, and have been uploaded on Vanta, to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Observed a screenshot of Mainstem's network diagram which indicates the key systems, hosts (e.g. database and application servers), and network information (e.g. IP addresses, network boundaries, VPNs, and bastion boxes) used to deliver a product or service, to determine that the company provides a description of its products and services to internal and external users. Observed the company's website (https://mainstem.zendesk.com/hc/en-us) which includes descriptions of the product features, pricing, and usage guidelines, to determine that the company provides a description of its products and services to internal and external users through its website.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and	The company communicates system changes to authorized internal users.	Observed a screenshot of an internal communication channel where users are notified about recent deployments, to determine that system changes are communicated to authorized internal users.	No exceptions noted.

	responsibilities for internal control, necessary to support the functioning of internal control.		Inspected the Operations Security Policy, which states that change management processes shall include advance communication and warning of changes, including schedules and a description of reasonably anticipated effects, to determine that the company communicates system changes to authorized internal users.	
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Observed that the company has an anonymous whistleblower channel at (https://docs.google.com/forms/d/e/1FAIpQLSeX0BKvvJnlt4X9bkTTDGn94jO1lYriDJRJB26PcLcy13TZ1w/viewform), which states that the user's email address will not be shared, to determine that an anonymous communication channel is in place for users to report potential issues or fraud concerns. Inspected the Information Security policy which states that all users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses to the email address "security@mainstem.io", to determine that the company has established an anonymous communication channel is in place for users to report potential issues or fraud concerns.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the Security Policy published on the company's website (https://www.mainstem.io/security/policy) which describes the company's annual penetration testing and SOC 2 audit requirements, to determine that the company's security commitments are communicated to customers through its online Security Policy. Inspected the Mainstem Inc Vendor MSA which includes confidentiality and non-compete clauses, to determine that the company's security commitments are communicated to customers in Master Service Agreements (MSA). Disclosure: There were no signed MSAs during the observation period.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the	The company notifies customers of critical system changes that may affect their processing.	Observed the company's application status page (https://status.mainstem.io/) which provides the historical and current uptime status along with a list of past incidents, to determine that the company notifies customers of critical system	No exceptions noted.

	functioning of internal control.		changes that may affect their processing. Observed the company's support page (https://support.mainstem.io/) which provides guidelines and assistance related to the company's services and features, to determine that the company notifies customers of critical system changes that may affect their processing through its website.	
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's website (https://www.mainstem.io/) which hosts various resources, including a blog, press releases, a newsroom, and a link to request a product demo, to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Observed a screenshot of Mainstem's network diagram which indicates the key systems, hosts (e.g. database and application servers), and network information (e.g. IP addresses, network boundaries, VPNs, and bastion boxes) used to deliver a product or service, to determine that the company provides a description of its products and services to internal and external users. Observed the company's website (https://mainstem.zendesk.com/hc/en-us) which includes descriptions of the product features, pricing, and usage guidelines, to determine that the company provides a description of its products and services to internal and external users through its website.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company 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.	Observed the support page on the company's website (https://support.mainstem.io/) which maintains a "Create Support Ticket" tab where customers submit a query to the management, to determine that a customer support system is available.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy	Inspected the online Microsoft Azure agreement (https://azure.microsoft.com/en-us/support/legal/) which includes clauses on data protection and privacy, to determine that the company's confidentiality and privacy commitments are documented in a vendor agreement.	No exceptions noted.

		commitments applicable to that entity.	Inspected the publicly available Terms and Conditions published on (https://www.mainstem.io/terms-conditions) which state the company's privacy and confidentiality commitments, to determine that the company's confidentiality and privacy commitments are communicated on a publicly available online Terms and Conditions page. Inspected the Privacy Policy of the company (https://www.mainstem.io/privacy-policy) which describes the privacy commitments of the company, including information collection and use practices, to determine that the company communicates its privacy requirements to vendors through its publicly available Privacy Policy.	
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy which states that the company has a risk management strategy, processes, and means to identify those risks that would hinder the achievement of its strategic and operational objectives to determine that the risk assessment objectives of the company are specified.	No exceptions noted.
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company 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.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing responses, to determine that the company has established a risk management program 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.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Mainstem Inc Incident Tabletop Exercise report, dated September 13, 2022, which describes the tabletop scenario, objectives, discussion questions, findings, and the results of a system recovery test, to determine that the company has a documented business	No exceptions noted.

	basis for determining how the risks should be managed.		continuity/disaster recovery (BC/DR) plan and tests it at least annually. Inspected the Business Continuity and Disaster Recovery Plan which states that a disaster recovery test shall be performed on an annual basis, to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan which is required to be tested at least annually.	
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company'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.	Observed through Vanta that a risk assessment has been completed within Vanta on August 9, 2022, to determine that the company's risk assessments are performed at least annually. Inspected the Risk Management Policy which states that a formal risk assessment is to be performed at least annually to determine that the company is required to perform annual risk assessments by identifying and assessing the environmental, regulatory, and technological threats to service delivery along with the risk of fraud.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company 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.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing responses, to determine that the company has established a risk management program 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.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and	Inspected the vendor directory maintained on Vanta which contains a list of vendors, along with their risk levels and compliance security assessment documents for the high-risk and medium-risk vendors, to determine that the company has a vendor management program in place which is managed through Vanta.	No exceptions noted.

	how the risks should be managed.	- review of critical third-party vendors at least annually.	Observed through Vanta that none of the listed vendors have an invalid review, to determine that the company conducts a review of critical third-party vendors at least annually. Inspected the Third Party Management Policy, which states the requirements for assessing supplier security and service delivery at least annually to determine that the company has a vendor management program.	
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company'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.	Observed through Vanta that a risk assessment has been completed within Vanta on August 9, 2022, to determine that the company's risk assessments are performed at least annually. Inspected the Risk Management Policy which states that a formal risk assessment is to be performed at least annually to determine that the company is required to perform annual risk assessments by identifying and assessing the environmental, regulatory, and technological threats to service delivery along with the risk of fraud.	No exceptions noted.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company 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.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing responses, to determine that the company has established a risk management program 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.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently	Observed a screenshot which shows a list of workflow runs with their current status, to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.

		throughout the environment.	Inspected the Operations Security Policy which states that all changes that may have a significant impact on information security, operations, or the production platform are required to be documented with managerial approval and authorization before proceeding, to determine that the company has established a configuration management system.	
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report submitted by Prescient Security on May 19, 2022, which describes the test details, testing tools, vulnerability details, methodology, prescribed remediations, and vulnerabilities and checks, to determine that the company's penetration testing is performed at least annually and a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the Operations Security Policy, which states that penetration tests of the applications and production network shall be performed annually, to determine that the company is required to perform annual penetration tests.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company'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.	Observed through Vanta that a risk assessment has been completed within Vanta on August 9, 2022, to determine that the company's risk assessments are performed at least annually. Inspected the Risk Management Policy which states that a formal risk assessment is to be performed at least annually to determine that the company is required to perform annual risk assessments by identifying and assessing the environmental, regulatory, and technological threats to service delivery along with the risk of fraud.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company 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	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing	No exceptions noted.

		identified threats, and mitigation strategies for those risks.	responses, to determine that the company has established a risk management program 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.	
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company 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.	Observed that the company uses Vanta for performing internal self-assessments on a continuous basis. Inspected the Risk Management Policy section titled "Practical Application of Risk Management" which states that the company shall review and update its risk assessment and perform an internal audit of the information security management system at least annually, and that security risks shall be evaluated at various stages of the software design and development lifecycle as needed, to determine that the company is required to perform annual control self-assessments.	No exceptions noted.
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report submitted by Prescient Security on May 19, 2022, which describes the test details, testing tools, vulnerability details, methodology, prescribed remediations, and vulnerabilities and checks, to determine that the company's penetration testing is performed at least annually and a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the Operations Security Policy, which states that penetration tests of the applications and production network shall be performed annually, to determine that the company is required to perform annual penetration tests.	No exceptions noted.
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor directory maintained on Vanta which contains a list of vendors, along with their risk levels and compliance security assessment documents for the high-risk and medium-risk vendors, to determine that the company has a vendor management program in place which is managed through Vanta. Observed through Vanta that none of the listed vendors have an invalid review, to determine that the company conducts a review of critical	No exceptions noted.

			third-party vendors at least annually. Inspected the Third Party Management Policy, which states the requirements for assessing supplier security and service delivery at least annually to determine that the company has a vendor management program.	
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, observed screenshots which show that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that critical and high vulnerabilities are tracked to remediation. Inspected the Operations Security Policy section titled "Technical Vulnerability Management" which states that external vulnerability scans are required to be run on the production environment at least quarterly, vulnerabilities should be evaluated, and appropriate measures should be taken to address the associated risks, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems, with critical and high vulnerabilities tracked to remediation.	No exceptions noted.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company 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.	Observed that the company uses Vanta for performing internal self-assessments on a continuous basis. Inspected the Risk Management Policy section titled "Practical Application of Risk Management" which states that the company shall review and update its risk assessment and perform an internal audit of the information security management system at least annually, and that security risks shall be evaluated at various stages of the software design and development lifecycle as needed, to determine that the company is required to perform annual control self-assessments.	No exceptions noted.

CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor directory maintained on Vanta which contains a list of vendors, along with their risk levels and compliance security assessment documents for the high-risk and medium-risk vendors, to determine that the company has a vendor management program in place which is managed through Vanta. Observed through Vanta that none of the listed vendors have an invalid review, to determine that the company conducts a review of critical third-party vendors at least annually. Inspected the Third Party Management Policy, which states the requirements for assessing supplier security and service delivery at least annually to determine that the company has a vendor management program.	No exceptions noted.
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company 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.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing responses, to determine that the company has established a risk management program 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.	No exceptions noted.
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy section titled "Management Responsibilities" which states that management shall be responsible for ensuring that the information security policies and procedures are reviewed annually and made accessible to all employees and contractors. Observed through Vanta that the Access Control Policy, Asset Management Policy, Cryptography Policy, and other policies were approved on August 07, 2022, and August 08, 2022, and have been uploaded on Vanta, to determine that the company's information security policies and	No exceptions noted.

			procedures are documented and reviewed at least annually.	
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company has established access control procedures. Inspected the Access Control Policy which describes the user access management procedures, including user registration, deregistration, and access provisioning, to determine that the company's Access Control Policy documents the requirements for adding new users, modifying users, and removing an existing user's access.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company 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.	Observed through Vanta that all employees have accepted the Secure Development Policy. Inspected the Secure Development Policy which provides system change control procedures and software version control guidelines, to determine that the company 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.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy section titled "Management Responsibilities" which states that management shall be responsible for ensuring that the information security policies and procedures are reviewed annually and made accessible to all employees and contractors. Observed through Vanta that the Access Control Policy, Asset Management Policy, Cryptography Policy, and other policies were approved on August 07, 2022, and August 08, 2022, and have been uploaded on Vanta, to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested,	Observed a screenshot which shows a list of workflow runs with their current status, to determine that the company has a change management procedure in place to ensure that system changes are deployed consistently throughout the environment.	No exceptions noted.

	in procedures that put policies into action.	reviewed, and approved prior to being implemented in the production environment.	Observed the data exported through Vanta which shows that all GitHub repositories require at least 1 approval to merge to the default branch, to determine that change management procedures are enforced at the company. Inspected the Operations Security Policy which describes the change management processes, including processes for planning and testing of changes, documenting managerial approval and authorization for changes, advance communication of changes to all relevant internal and external stakeholders, documentation of all emergency changes and subsequent reviews, and a process for remediating unsuccessful changes, to determine that the company 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.	
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Mainstem Inc Tabletop Exercise report dated September 13, 2022, which includes an assessment of the data backup and recovery plans, to determine that backup processes have been established at the company. Inspected the Operations Security Policy section titled "Information Backup" which states that backups on in-scope systems are configured to run daily, to determine that the company's data backup policy documents requirements for backup and recovery of customer data.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Observed through Vanta that all relevant employees have agreed to the Data Management Policy. Inspected the Data Management Policy's section titled "Data Retention" which states that customer data may be retained as long as the company has a need for its use, or to meet regulatory or contractual requirements and that once data is no longer needed, it shall be securely disposed of or archived whereas the retention periods are to be determined by data owners in consultation with legal counsel, to determine that the company has formal retention and disposal procedures in place	No exceptions noted.

			to guide the secure retention and disposal of company and customer data.	
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company 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.	Observed through Vanta that all employees have accepted the Secure Development Policy. Inspected the Secure Development Policy which provides system change control procedures and software version control guidelines, to determine that the company 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.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Observed through Vanta that all relevant employees have accepted the Incident Response Plan to determine that the plan is communicated to authorized users. Inspected the Incident Response Plan which provides guidance for reporting, categorizing, escalating, and documenting security incidents, the steps to be followed in responding to an incident, and the roles and responsibilities of response team members, to determine that security and privacy incident response policies have been documented by the management.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy which states that the company has a risk management strategy, processes, and means to identify those risks that would hinder the achievement of its strategic and operational objectives to determine that the risk assessment objectives of the company are specified.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company 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	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing responses, to determine that the company has	No exceptions noted.

		mitigation strategies for those risks.	established a risk management program 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.	
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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.	Observed through Vanta that all relevant employees have accepted the Information Security Roles and Responsibilities Policy, to determine that the employees have accepted the roles and responsibilities for information security. Inspected the Information Security Roles and Responsibilities Policy section titled "Audience" which states that the employees and contractors of the company are responsible for acting at all times in a manner that does not place at risk the health and safety of themselves, other people in the workplace, and the information and resources they have use of, helping to identify areas where risk management practices should be adopted, taking all practical steps to minimize the company's exposure to contractual and regulatory liability, adhering to company policies and standards of conduct and reporting incidents and observed anomalies or weaknesses to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy section titled "Management Responsibilities" which states that management shall be responsible for ensuring that the information security policies and procedures are reviewed annually and made accessible to all employees and contractors. Observed through Vanta that the Access Control Policy, Asset Management Policy, Cryptography Policy, and other policies were approved on August 07, 2022, and August 08, 2022, and have been uploaded on Vanta, to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.

CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor directory maintained on Vanta which contains a list of vendors, along with their risk levels and compliance security assessment documents for the high-risk and medium-risk vendors, to determine that the company has a vendor management program in place which is managed through Vanta. Observed through Vanta that none of the listed vendors have an invalid review, to determine that the company conducts a review of critical third-party vendors at least annually. Inspected the Third Party Management Policy, which states the requirements for assessing supplier security and service delivery at least annually to determine that the company has a vendor management program.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the application to authorized users with a business need.	Observed the data exported from Vanta which shows that all employees have unique email accounts, unique AWS accounts with a specific role, and unique GitHub accounts, to determine that the company restricts privileged access to the application to authorized users with a business need. Observed through Vanta that every AWS group has at least one IAM policy attached, employee account permissions are managed by AWS groups, and no AWS IAM policies are attached directly to users, to determine that production application access is restricted at the company. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege, to determine that the company restricts privileged access to the application to authorized users with a business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company has established access control procedures. Inspected the Access Control Policy which describes the user access management procedures, including user registration, deregistration, and	No exceptions noted.

	to meet the entity's objectives.	- removing an existing user's access.	access provisioning, to determine that the company's Access Control Policy documents the requirements for adding new users, modifying users, and removing an existing user's access.	
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to databases to authorized users with a business need.	Observed the data exported from Vanta which shows that all employees have unique email accounts, unique AWS accounts with a specific role, and unique GitHub accounts, to determine that the company restricts privileged access to the database to authorized users with a business need. Observed the data exported from Vanta which shows that all relevant AWS accounts have been linked to users within Vanta, to determine that the company restricts privileged access to databases to authorized users with business needs. Inspected the Access Control Policy which states that Mainstem Inc shall determine the type and level of access granted to individual users based on the ,principle of least privilege, and Role-Based Access Control (RBAC), to determine that the company restricts privileged access to the database to authorized users with a business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Observed the data exported through Vanta which shows that MFA is enabled on all relevant GitHub and AWS user accounts, to determine that the company enforces unique production database authentication. Inspected the Access Control Policy which states that the company requires all privileged access to production systems to use Multi-Factor Authentication (MFA), to determine that the company is required to enforce unique production database authentication.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the Cryptography Policy's section titled "Key Management" which states that access to keys and secrets such as web ciphers and passwords is to be tightly controlled in accordance with the Access Control Policy, to determine that the company restricts access to encryption keys. Observed the company's AWS IAM user list to determine that the company restricts access to encryption keys to authorized users.	No exceptions noted.

CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Observed the data exported from Vanta which shows that public SSH is denied and all AWS EC2 instances have network ACLs or security groups attached, to determine that the company restricts privileged access to the firewall to authorized users with a business need. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege to determine that the company restricts privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the operating system to authorized users with a business need.	Observed the data exported from Vanta which shows that all relevant AWS accounts have been linked to users within Vanta, and all users have unique AWS accounts with a specific role, to determine that the company restricts privileged access to the operating system to authorized users with a business need. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege to determine that the company restricts privileged access to the production OS to authorized users with a business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the production network to authorized users with a business need.	Observed the data exported from Vanta which shows that all AWS accounts have been linked to users within Vanta who have production network access, and all users have unique AWS accounts with a specific role, to determine that the company restricts privileged access to the production network to authorized users with a business need. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege to determine that the company restricts privileged access to the network to authorized users with a business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over	The company ensures that user access to in-scope system components is based on job role and function or requires a	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a	No exceptions noted.

	protected information assets to protect them from security events to meet the entity's objectives.	documented access request form and manager approval prior to access being provisioned.	documented access request form and manager approval prior to access being provisioned. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege and role-based access, to determine that access requests are required in order to grant users access to in-scope system components.	
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed the data exported from Vanta which shows that the password policy configured for AWS requires a minimum password length of 6 characters, including uppercase letters, lowercase letters, symbols, and numbers, to determine that the company requires authentication to the "production network" to use unique usernames and passwords. Observed that all employees have unique email IDs, AWS accounts, and GitHub accounts, to determine that unique accounts and passwords are required to access the network system.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts access to migrate changes to production to authorized personnel.	Observed the data exported through Vanta which shows that all linked version control repositories require at least 1 approval to merge to the default master branch, to determine that the company restricts access to migrate changes to production to authorized personnel. Observed through Vanta that at least one repository in the linked version control system has been updated in the last 30 days, to determine that GitHub deployment access is restricted at the company. Inspected the "Software Version Control" section of the Secure Development Policy which states that all software is version controlled and synced between contributors (developers) and access to the central repository is restricted based on an employee's role, to determine that production deployment access is restricted.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over	The company has a data classification policy in place to help ensure that confidential data is properly secured and	Observed through Vanta that all relevant employees have accepted the Data Management Policy, to determine that the company has a data classification policy in place.	No exceptions noted.

	protected information assets to protect them from security events to meet the entity's objectives.	restricted to authorized personnel.	Inspected the Data Management Policy section titled "Data Classification" which establishes the rules for categorizing data as confidential, restricted, and public depending on its criticality and the need to protect it and also prescribes appropriate data labeling and handling procedures for each type, to determine that the company has a data classification policy in place.	
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Observed through Vanta that all Cosmo DB databases and SQL databases are encrypted, to determine that the company's datastores housing sensitive customer data are encrypted at rest. Inspected the Cryptography Policy which states that the company shall implement cryptographic controls to mitigate data risks where deemed appropriate, to determine that the company is required to implement data encryption.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's network is segmented to prevent unauthorized access to customer data.	Observed the data exported through Vanta which shows a list of network security groups that contain inbound and outbound security rules, to determine that the company's network is segmented to prevent unauthorized access to customer data. Observed the data exported through Vanta which shows a list of AD security groups, to determine that the company's network is segmented.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Observed through Vanta that all employees with the Vanta Agent installed have a password manager installed and that all AWS accounts have password policies enabled, to determine that password policies are implemented. Observed the data exported from Vanta which shows the password policy configured for AWS requiring a minimum password length of 6 characters, including uppercase, lowercase, numbers, and symbols, to determine that the password policy of the company has been enforced. Observed through Vanta that all employees with Microsoft Endpoint Manager have a password manager installed, to determine that password policies are implemented through a password manager.	No exceptions noted.

CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Inspected the production inventory list, exported from Vanta, which contains all the Azure, GitHub, AWS S3, and Microsoft Endpoint assets, with their respective owners and descriptions, to determine that the company maintains a formal inventory of production system assets. Inspected the Asset Management Policy which states that assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified, and an inventory of these assets shall be drawn up and maintained, to determine that the company is required to maintain a formal inventory of production system assets.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Observed the data exported from Vanta which shows that MFA is enabled on all relevant AWS user, AWS root, and GitHub accounts, to determine that remote access MFA is enforced. Inspected the Information Security Policy which states that the use of remote access software and services is allowable as long as it is provided by the company and configured for multi-factor authentication (MFA), to determine that the company requires MFA to be implemented for user's access its resources remotely.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Observed the validity of the security certificate of the website (https://www.mainstem.io/) which is valid up to November 29, 2022, to determine that remote access is encrypted and enforced. Inspected the Access Control Policy which states that remote connections to production systems and networks must be encrypted, to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Observed the data exported from Vanta which shows that all employees have unique email IDs and GitHub accounts, to determine that the company requires authentication to systems and applications to use unique usernames and passwords. Observed that employee AWS account permissions are managed by AWS groups, every AWS account	No exceptions noted.

	to meet the entity's objectives.		has been assigned a role, and no user account has a policy attached directly, to determine that unique account authentication is enforced.	
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company has established access control procedures. Inspected the Access Control Policy which describes the user access management procedures, including user registration, deregistration, and access provisioning, to determine that the company's Access Control Policy documents the requirements for adding new users, modifying users, and removing an existing user's access.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company 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.	Inspected the Access Review Report dated September 14, 2022, which shows the access reviews for Microsoft 365, GitHub, Jira, Gusto, LastPass, and Azure accounts, to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Observed screenshot of access reviews of Microsoft 365, LastPass, Jira, Gusto, GitHub, and Azure users, which shows the active users and admins, to determine that the company conducts access reviews at least quarterly for the in-scope system components. Observed the data exported from Vanta which shows that all GitHub, AWS, HR, and Jira infrastructure accounts are linked to users and Vanta, to determine that the company conducts access reviews at least quarterly for the in-scope system components.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected an employee termination checklist which includes the requirement to deactivate logical access to various systems, including GitHub, Azure, Office, and Jira, to determine that the company revokes user access upon termination.	No exceptions noted.

	internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		Observed through Vanta that all user accounts of AWS, GitHub, and Jira are deprovisioned and users are removed within the specified SLA, to determine that the company revokes user access upon termination.	
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company 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.	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company 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. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege and role-based access, to determine that access requests are required in order to grant users access to in-scope system components.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed the data exported from Vanta which shows that the password policy configured for AWS requires a minimum password length of 6 characters, including uppercase letters, lowercase letters, symbols, and numbers, to determine that the company requires authentication to the "production network" to use unique usernames and passwords. Observed that all employees have unique email IDs, AWS accounts, and GitHub accounts, to determine that unique accounts and passwords are required to access the network system.	No exceptions noted.

CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company has established access control procedures. Inspected the Access Control Policy which describes the user access management procedures, including user registration, deregistration, and access provisioning, to determine that the company's Access Control Policy documents the requirements for adding new users, modifying users, and removing an existing user's access.	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company 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.	Inspected the Access Review Report dated September 14, 2022, which shows the access reviews for Microsoft 365, GitHub, Jira, Gusto, LastPass, and Azure accounts, to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Observed screenshot of access reviews of Microsoft 365, LastPass, Jira, Gusto, GitHub, and Azure users, which shows the active users and admins, to determine that the company conducts access reviews at least quarterly for the in-scope system components. Observed the data exported from Vanta which shows that all GitHub, AWS, HR, and Jira infrastructure accounts are linked to users and Vanta, to determine that the company conducts access reviews at least quarterly for the in-scope system components.	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected an employee termination checklist which includes the requirement to deactivate logical access to various systems, including GitHub, Azure, Office, and Jira, to determine that the company revokes user access upon termination. Observed through Vanta that all user accounts of AWS, GitHub, and Jira are deprovisioned and users are removed within the specified SLA, to	No exceptions noted.

	consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		determine that the company revokes user access upon termination.	
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company 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.	Observed screenshots of two user access requests sent by the respective users' managers, which were accepted, to determine that the company 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. Inspected the Access Control Policy which states that the company is required to give privileged access to users based on the principle of least privilege and role-based access, to determine that access requests are required in order to grant users access to in-scope system components.	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed the data exported from Vanta which shows that the password policy configured for AWS requires a minimum password length of 6 characters, including uppercase letters, lowercase letters, symbols, and numbers, to determine that the company requires authentication to the "production network" to use unique usernames and passwords. Observed that all employees have unique email IDs, AWS accounts, and GitHub accounts, to determine that unique accounts and passwords are required to access the network system.	No exceptions noted.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to	The company 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.	Inspected the Access Review Report dated September 14, 2022, which shows the access reviews for Microsoft 365, GitHub, Jira, Gusto, LastPass, and Azure accounts, to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Observed screenshot of access reviews of	No exceptions noted.

	authorized personnel to meet the entity's objectives.		Microsoft 365, LastPass, Jira, Gusto, GitHub, and Azure users, which shows the active users and admins, to determine that the company conducts access reviews at least quarterly for the in-scope system components. Observed the data exported from Vanta which shows that all GitHub, AWS, HR, and Jira infrastructure accounts are linked to users and Vanta, to determine that the company conducts access reviews at least quarterly for the in-scope system components.	
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected an employee termination checklist which includes the requirement to deactivate logical access to various systems, including GitHub, Azure, Office, and Jira, to determine that the company revokes user access upon termination. Observed through Vanta that all user accounts of AWS, GitHub, and Jira are deprovisioned and users are removed within the specified SLA, to determine that the company revokes user access upon termination.	No exceptions noted.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company 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 to determine that hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed. Disclosure: The company has not disposed of any assets during the observation period.	No exceptions noted.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Management Policy to determine that customer accounts and data shall be deleted within sixty (60) days of contract termination through manual data deletion processes. Disclosure: The company has not received any data deletion requests from customers during the observation period.	No exceptions noted.

	diminished and is no longer required to meet the entity's objectives.			
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Observed through Vanta that all relevant employees have agreed to the Data Management Policy. Inspected the Data Management Policy's section titled "Data Retention" which states that customer data may be retained as long as the company has a need for its use, or to meet regulatory or contractual requirements and that once data is no longer needed, it shall be securely disposed of or archived whereas the retention periods are to be determined by data owners in consultation with legal counsel, to determine that the company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed the data exported from Vanta which shows that the password policy configured for AWS requires a minimum password length of 6 characters, including uppercase letters, lowercase letters, symbols, and numbers, to determine that the company requires authentication to the "production network" to use unique usernames and passwords. Observed that all employees have unique email IDs, AWS accounts, and GitHub accounts, to determine that unique accounts and passwords are required to access the network system.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Observed that the security certificate of the website (https://www.mainstem.io/) is valid up to November 29, 2022, strong SSL/TLS cipher codes are implemented, and HTTP is redirected to HTTPS via a 3XX status code, to determine that remote access is encrypted and enforced. Inspected the Data Management Policy which states that confidential information may only be transmitted over the public Internet by using TLS v1.2 or a better protocol, to determine that data transmission is required to be encrypted.	No exceptions noted.

CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Observed through Vanta that the company uses GuardDuty for intrusion detection. Observed through Vanta that all employees required to install Vanta Agent have installed it on their workstations and that all linked AWS accounts have CloudTrail enabled, to determine that employee workstations are monitored with Vanta. Observed screenshots which show that S3 protection, Kubernetes audit log monitoring, and malware protection are enabled on GuardDuty, to determine that GuardDuty is used for intrusion detection.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Observed through Vanta that the company uses AWS which has a built-in firewall feature that is reviewed and updated as per AWS's policies. Observed the data exported from Vanta which demonstrates that Azure Security Group is attached and unwanted traffic is filtered on AWS and public SSH is denied, to determine that firewalls are utilized and reviewed.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Observed through Vanta that the company uses AWS which has a built-in firewall feature and Azure security groups are attached which filters unrestricted access to TCP port 22, to determine that network firewalls are utilized to prevent unauthorized access.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Observed the data exported from Vanta which shows that MFA is enabled on all relevant AWS user, AWS root, and GitHub accounts, to determine that remote access MFA is enforced. Inspected the Information Security Policy which states that the use of remote access software and services is allowable as long as it is provided by the company and configured for multi-factor authentication (MFA), to determine that the company requires MFA to be implemented for user's access its resources remotely.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Observed the validity of the security certificate of the website (https://www.mainstem.io/) which is valid up to November 29, 2022, to determine that remote access is encrypted and enforced. Inspected the Access Control Policy which states	No exceptions noted.

			that remote connections to production systems and networks must be encrypted, to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company 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.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, and that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that the service infrastructure is maintained. Observed through Vanta that the company documents security issues through a 'security' tag and assigns them a priority level in Jira, to determine that the company maintains its service infrastructure regularly.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Observed the data through Vanta which shows that the company uses AWS which maintains an industry-level network and system hardening and security standards. Observed through Vanta that all AWS accounts have been linked to users within Vanta, and all AWS EC2 instances have network ACLs or security groups attached, to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually in line with AWS policies.	No exceptions noted.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Observed through Vanta that all employees have hard disk encryption enabled on their operating system workstations to determine that portable media are encrypted. Observed a screenshot of Windows OS which shows that hard disk encryption is enabled using BitLocker, to determine that the company encrypts portable and removable media devices when used.	No exceptions noted.
CC 6.7	The entity restricts the transmission, movement, and	The company uses secure data transmission protocols to encrypt confidential and	Observed that the security certificate of the website (https://www.mainstem.io/) is valid up to November 29, 2022, strong SSL/TLS cipher codes	No exceptions noted.

	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.	sensitive data when transmitted over public networks.	are implemented, and HTTP is redirected to HTTPS via a 3XX status code, to determine that remote access is encrypted and enforced. Inspected the Data Management Policy which states that confidential information may only be transmitted over the public Internet by using TLS v1.2 or a better protocol, to determine that data transmission is required to be encrypted.	
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.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Observed that the company uses Vanta as an MDM. Inspected the Information Security Policy section titled "Mobile Device Policy" which states that all end-user devices (mobile phones, tablets, laptops, desktops) must comply with the Device Policy, to determine that the company has Mobile Device Management (MDM) system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity, objectives.	The company 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.	Observed through Vanta that all employees with Windows OS have antivirus software installed on their systems, to determine that the company 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. Inspected the Operations Security Policy which states that detection, prevention, and recovery controls to protect the company's systems and networks against malware shall be implemented, combined with appropriate user awareness, to determine that the company is required to use anti-malware technology.	No exceptions noted.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity, objectives.	The company 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.	Observed through Vanta that all employees have accepted the Secure Development Policy. Inspected the Secure Development Policy which provides system change control procedures and software version control guidelines, to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency	No exceptions noted.

			changes), and maintenance of information systems and related technology requirements.	
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity, objectives.	The company 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.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, and that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that the service infrastructure is maintained. Observed through Vanta that the company documents security issues through a 'security' tag and assigns them a priority level in Jira, to determine that the company maintains its service infrastructure regularly.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company 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.	Observed a screenshot which shows a list of workflow runs with their current status, to determine that the company has a change management procedure in place to ensure that system changes are deployed consistently throughout the environment. Observed the data exported through Vanta which shows that all GitHub repositories require at least 1 approval to merge to the default branch, to determine that change management procedures are enforced at the company. Inspected the Operations Security Policy which describes the change management processes, including processes for planning and testing of changes, documenting managerial approval and authorization for changes, advance communication of changes to all relevant internal and external stakeholders, documentation of all emergency changes and subsequent reviews, and a process for remediating unsuccessful changes, to determine that the company 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.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures	The company has a configuration management procedure in place to ensure that system	Observed a screenshot which shows a list of workflow runs with their current status, to determine that the company has a configuration management procedure in place to ensure that	No exceptions noted.

	to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	configurations are deployed consistently throughout the environment.	system configurations are deployed consistently throughout the environment. Inspected the Operations Security Policy which states that all changes that may have a significant impact on information security, operations, or the production platform are required to be documented with managerial approval and authorization before proceeding, to determine that the company has established a configuration management system.	
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy which places primary responsibility for evaluating the severity of vulnerabilities and issuing tickets on the IT and Engineering departments, to determine that vulnerability management and system monitoring procedures are established. Observed that the Operations Security Policy provides guidelines for issuing tickets along with the estimated remediation timeframes for critical, high, medium, low, and informational severity, to determine that vulnerability management procedures are established at the company.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company'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.	Observed through Vanta that a risk assessment has been completed within Vanta on August 9, 2022, to determine that the company's risk assessments are performed at least annually. Inspected the Risk Management Policy which states that a formal risk assessment is to be performed at least annually to determine that the company is required to perform annual risk assessments by identifying and assessing the environmental, regulatory, and technological threats to service delivery along with the risk of fraud.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, observed screenshots which show that a	No exceptions noted.

	vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that critical and high vulnerabilities are tracked to remediation. Inspected the Operations Security Policy section titled "Technical Vulnerability Management" which states that external vulnerability scans are required to be run on the production environment at least quarterly, vulnerabilities should be evaluated, and appropriate measures should be taken to address the associated risks, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems, with critical and high vulnerabilities tracked to remediation.	
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Observed through Vanta that the company uses GuardDuty for intrusion detection. Observed through Vanta that all employees required to install Vanta Agent have installed it on their workstations and that all linked AWS accounts have CloudTrail enabled, to determine that employee workstations are monitored with Vanta. Observed screenshots which show that S3 protection, Kubernetes audit log monitoring, and malware protection are enabled on GuardDuty, to determine that GuardDuty is used for intrusion detection.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Observed the data exported through Vanta which shows that Office, Jira, Azure, Microsoft Endpoint Manager, GitHub, AWS, Checkr, Gusto, and Confluence infrastructures are linked to Vanta, to determine that activity on these applications is tracked on Vanta. Observed through Vanta that all linked AWS accounts have CloudTrial enabled, Azure security groups have flow logs enabled, AWS S3 server logs are enabled with access allowed only to authorized users, AWS CloudWatch Log Groups retain logs for at least 365 days, and VPC flow logs are enabled, to determine that logging is performed at the company on a regular basis.	No exceptions noted.

			Inspected the Operations Security Policy's section titled "Logging & Monitoring" which states that production infrastructure is to be configured to produce detailed event logs appropriate to the function served by the system or device, including user activity, exceptions, faults, and information security events, to determine that the company is required to utilize log management.	
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report submitted by Prescient Security on May 19, 2022, which describes the test details, testing tools, vulnerability details, methodology, prescribed remediations, and vulnerabilities and checks, to determine that the company's penetration testing is performed at least annually and a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the Operations Security Policy, which states that penetration tests of the applications and production network shall be performed annually, to determine that the company is required to perform annual penetration tests.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy which places primary responsibility for evaluating the severity of vulnerabilities and issuing tickets on the IT and Engineering departments, to determine that vulnerability management and system monitoring procedures are established. Observed that the Operations Security Policy provides guidelines for issuing tickets along with the estimated remediation timeframes for critical, high, medium, low, and informational severity, to determine that vulnerability management procedures are established at the company.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, and that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that the service infrastructure is maintained.	No exceptions noted.

	the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	supporting the service are hardened against security threats.	Observed through Vanta that the company documents security issues through a 'security' tag and assigns them a priority level in Jira, to determine that the company maintains its service infrastructure regularly.	
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Observed through Vanta that AWS accounts have at least one active load balancer, whereas all AWS load balancer activity, unhealthy host count, latency, server errors, and I/O database activity are monitored via Azure, to determine that infrastructure monitoring tools are utilized to monitor systems, infrastructure, and performance.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, observed screenshots which show that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that critical and high vulnerabilities are tracked to remediation. Inspected the Operations Security Policy section titled "Technical Vulnerability Management" which states that external vulnerability scans are required to be run on the production environment at least quarterly, vulnerabilities should be evaluated, and appropriate measures should be taken to address the associated risks, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems, with critical and high vulnerabilities tracked to remediation.	No exceptions noted.

CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Observed through Vanta that all relevant employees have accepted the Incident Response Plan to determine that the plan is communicated to authorized users. Inspected the Incident Response Plan which provides guidance for reporting, categorizing, escalating, and documenting security incidents, the steps to be followed in responding to an incident, and the roles and responsibilities of response team members, to determine that security and privacy incident response policies have been documented by the management.	No exceptions noted.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan, which states the steps to be followed in responding to an incident, and the roles and responsibilities of the response team members, to determine that the management is required to follow the incident management procedures for logging, tracking, resolving, and communicating the results to the affected or relevant parties. Disclosure: There were no incidents during the observation period.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests their incident response plan at least annually.	Inspected the Incident Tabletop Exercise document, dated September 13, 2022, which describes a scenario for testing the incident response plan, to determine that the company tests its incident response plan at least annually.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Observed through Vanta that all relevant employees have accepted the Incident Response Plan to determine that the plan is communicated to authorized users. Inspected the Incident Response Plan which provides guidance for reporting, categorizing, escalating, and documenting security incidents, the steps to be followed in responding to an incident, and the roles and responsibilities of response team members, to determine that security and privacy incident response policies have been documented by the management.	No exceptions noted.

CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan, which states the steps to be followed in responding to an incident, and the roles and responsibilities of the response team members, to determine that the management is required to follow the incident management procedures for logging, tracking, resolving, and communicating the results to the affected or relevant parties. Disclosure: There were no incidents during the observation period.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company 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.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, and that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that the service infrastructure is maintained. Observed through Vanta that the company documents security issues through a 'security' tag and assigns them a priority level in Jira, to determine that the company maintains its service infrastructure regularly.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, observed screenshots which show that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that critical and high vulnerabilities are tracked to remediation. Inspected the Operations Security Policy section titled "Technical Vulnerability Management" which states that external vulnerability scans are required to be run on the production environment at least quarterly, vulnerabilities should be evaluated, and appropriate measures should be taken to address the associated risks, to determine that host-based vulnerability scans are performed	No exceptions noted.

			at least quarterly on all external-facing systems, with critical and high vulnerabilities tracked to remediation.	
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Mainstem Inc Incident Tabletop Exercise report, dated September 13, 2022, which describes the tabletop scenario, objectives, discussion questions, findings, and the results of a system recovery test, to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. Inspected the Business Continuity and Disaster Recovery Plan which states that a disaster recovery test shall be performed on an annual basis, to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan which is required to be tested at least annually.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the Incident Tabletop Exercise document, dated September 13, 2022, which describes a scenario for testing the incident response plan, to determine that the company tests its incident response plan at least annually.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Observed through Vanta that all relevant employees have accepted the Incident Response Plan to determine that the plan is communicated to authorized users. Inspected the Incident Response Plan which provides guidance for reporting, categorizing, escalating, and documenting security incidents, the steps to be followed in responding to an incident, and the roles and responsibilities of response team members, to determine that security and privacy incident response policies have been documented by the management.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan, which states the steps to be followed in responding to an incident, and the roles and responsibilities of the response team members, to determine that the management is required to follow the incident management procedures for logging, tracking, resolving, and communicating the results to the affected or relevant parties.	No exceptions noted.

			Disclosure: There were no incidents during the observation period.	
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company 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.	Observed a screenshot which shows a list of workflow runs with their current status, to determine that the company has a change management procedure in place to ensure that system changes are deployed consistently throughout the environment. Observed the data exported through Vanta which shows that all GitHub repositories require at least 1 approval to merge to the default branch, to determine that change management procedures are enforced at the company. Inspected the Operations Security Policy which describes the change management processes, including processes for planning and testing of changes, documenting managerial approval and authorization for changes, advance communication of changes to all relevant internal and external stakeholders, documentation of all emergency changes and subsequent reviews, and a process for remediating unsuccessful changes, to determine that the company 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.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company restricts access to migrate changes to production to authorized personnel.	Observed the data exported through Vanta which shows that all linked version control repositories require at least 1 approval to merge to the default master branch, to determine that the company restricts access to migrate changes to production to authorized personnel. Observed through Vanta that at least one repository in the linked version control system has been updated in the last 30 days, to determine that GitHub deployment access is restricted at the company. Inspected the "Software Version Control" section of the Secure Development Policy which states that all software is version controlled and synced between contributors (developers) and access to the central repository is restricted based on an	No exceptions noted.

			employee's role, to determine that production deployment access is restricted.	
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company 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.	Observed through Vanta that all employees have accepted the Secure Development Policy. Inspected the Secure Development Policy which provides system change control procedures and software version control guidelines, to determine that the company 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.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report submitted by Prescient Security on May 19, 2022, which describes the test details, testing tools, vulnerability details, methodology, prescribed remediations, and vulnerabilities and checks, to determine that the company's penetration testing is performed at least annually and a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the Operations Security Policy, which states that penetration tests of the applications and production network shall be performed annually, to determine that the company is required to perform annual penetration tests.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company 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.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, and that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that the service infrastructure is maintained. Observed through Vanta that the company documents security issues through a 'security' tag and assigns them a priority level in Jira, to determine that the company maintains its service infrastructure regularly.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests,	The company's network and system hardening standards are documented, based on industry best practices,	Observed the data through Vanta which shows that the company uses AWS which maintains an industry-level network and system hardening and security standards.	No exceptions noted.

	approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	and reviewed at least annually.	Observed through Vanta that all AWS accounts have been linked to users within Vanta, and all AWS EC2 instances have network ACLs or security groups attached, to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually in line with AWS policies.	
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed a screenshot which shows that all identified vulnerabilities have been closed and that there are no open Dependabot alerts, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, observed screenshots which show that a vulnerability detected by Dependabot was assigned a high priority level, and was resolved by the risk owner with an appropriate commit, to determine that critical and high vulnerabilities are tracked to remediation. Inspected the Operations Security Policy section titled "Technical Vulnerability Management" which states that external vulnerability scans are required to be run on the production environment at least quarterly, vulnerabilities should be evaluated, and appropriate measures should be taken to address the associated risks, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems, with critical and high vulnerabilities tracked to remediation.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company 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.	Inspected the Business Continuity and Disaster Recovery Plan's section titled "Communications and Escalation" which requires executive staff and senior managers to be notified of any disaster affecting the company's facilities or operations and communications to take place over any available regular channels including Teams, to determine that the company has established Business Continuity and Disaster Recovery procedures, especially communication plans, to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.

			Observed through Vanta that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan.	
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Observed a screenshot which shows that the company has procured network security coverage from the Scottsdale Insurance Company, which is valid until December 31, 2022, to determine that the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions. Inspected the Risk Management Policy section titled "Risk Response and Treatment" which states that the company may use insurance as protection against financial loss, to determine that the company has the option to purchase a cybersecurity insurance policy.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company'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.	Observed through Vanta that a risk assessment has been completed within Vanta on August 9, 2022, to determine that the company's risk assessments are performed at least annually. Inspected the Risk Management Policy which states that a formal risk assessment is to be performed at least annually to determine that the company is required to perform annual risk assessments by identifying and assessing the environmental, regulatory, and technological threats to service delivery along with the risk of fraud.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company 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.	Observed through Vanta that all employees have acknowledged the Risk Management Policy. Inspected the Risk Management Policy sections titled "Risk Management Strategy" and "Risk Management Procedure" which outline the criteria and processes of maintaining a risk register and treatment plan, ranking and assessing risks, analyzing their impact, and implementing responses, to determine that the company has established a risk management program 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.	No exceptions noted.

CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the online Microsoft Azure agreement (https://azure.microsoft.com/en-us/support/legal/) which includes clauses on data protection and privacy, to determine that the company's confidentiality and privacy commitments are documented in a vendor agreement. Inspected the publicly available Terms and Conditions published on (https://www.mainstem.io/terms-conditions) which state the company's privacy and confidentiality commitments, to determine that the company's confidentiality and privacy commitments are communicated on a publicly available online Terms and Conditions page. Inspected the Privacy Policy of the company (https://www.mainstem.io/privacy-policy) which describes the privacy commitments of the company, including information collection and use practices, to determine that the company communicates its privacy requirements to vendors through its publicly available Privacy Policy.	No exceptions noted.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor directory maintained on Vanta which contains a list of vendors, along with their risk levels and compliance security assessment documents for the high-risk and medium-risk vendors, to determine that the company has a vendor management program in place which is managed through Vanta. Observed through Vanta that none of the listed vendors have an invalid review, to determine that the company conducts a review of critical third-party vendors at least annually. Inspected the Third Party Management Policy, which states the requirements for assessing supplier security and service delivery at least annually to determine that the company has a vendor management program.	No exceptions noted.