System and Organization Controls Report (SOC 2® Type 1)

Report on Model Evaluation and Threat Research, Inc.'s Description of Its Production Inspect Action Platform and on the Suitability of the Design of Its Controls Relevant to Security as of August 1, 2025

METR

INSIGHT ASSURANCE

☎ +1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR’S REPORT 1

INDEPENDENT SERVICE AUDITOR’S REPORT 2

SECTION 2: MODEL EVALUATION AND THREAT RESEARCH, INC.’S MANAGEMENT ASSERTION 5

MODEL EVALUATION AND THREAT RESEARCH, INC.’S MANAGEMENT ASSERTION 6

SECTION 3: MODEL EVALUATION AND THREAT RESEARCH, INC.’S DESCRIPTION OF ITS PRODUCTION INSPECT ACTION PLATFORM 7

MODEL EVALUATION AND THREAT RESEARCH, INC.’S DESCRIPTION OF ITS PRODUCTION INSPECT ACTION PLATFORM 8

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS 21

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 23

CONTROL ENVIRONMENT 23

COMMUNICATION AND INFORMATION 25

RISK ASSESSMENT 27

MONITORING ACTIVITIES 29

CONTROL ACTIVITIES 30

LOGICAL AND PHYSICAL ACCESS CONTROLS 32

SYSTEM OPERATIONS 36

CHANGE MANAGEMENT 39

RISK MITIGATION 40

SECTION 1:
INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Model Evaluation and Threat Research, Inc.

Scope

We have examined Model Evaluation and Threat Research, Inc.'s ("METR" or "the service organization") accompanying description of its Production Inspect Action Platform found in Section 3 titled "Model Evaluation and Threat Research, Inc.'s description of its Production Inspect Action Platform" as of August 1, 2025, ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of August 1, 2025, to provide reasonable assurance that METR's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

METR uses Amazon Web Services ("AWS" or "subservice organization") to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at METR, to achieve METR's service commitments and system requirements based on the applicable trust services criteria. The description presents METR's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of METR'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.

Service Organization's Responsibilities

METR is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that METR's service commitments and system requirements would be achieved. In Section 2, METR has provided the accompanying assertion titled "Model Evaluation and Threat Research, Inc.'s Management Assertion" (assertion) about the description and the suitability of the design of controls stated therein. METR 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 the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 to provide reasonable assurance that the service organization’s service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of a description of a service organization’s system and the suitability of the design of controls involves—

- obtaining an understanding of the system and the service organization’s service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

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. The projection to the future of any conclusions about the suitability of the design 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,

- the description presents METR’s Production Inspect Action Platform that was designed and implemented as of August 1, 2025, in accordance with the description criteria.

- the controls stated in the description were suitably designed as of August 1, 2025, to provide reasonable assurance that METR's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date and if the subservice organization applied the complementary controls assumed in the design of METR's controls as of that date.

Restricted Use

This report is intended solely for the information and use of management of METR; user entities of METR's Production Inspect Action Platform as of August 1, 2025; business partners of METR subject to risks arising from interactions with the Production Inspect Action Platform; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

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

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

Insight Assurance LLC

Tampa, Florida
December 16, 2025

SECTION 2:
MODEL EVALUATION AND THREAT RESEARCH, INC.’S MANAGEMENT ASSERTION

METR

MODEL EVALUATION AND THREAT RESEARCH, INC.’S MANAGEMENT ASSERTION

We have prepared the description of Model Evaluation and Threat Research, Inc.’s (“METR” or “the service organization”) Production Inspect Action Platform entitled “Model Evaluation and Threat Research, Inc.’s description of its Production Inspect Action Platform” as of August 1, 2025, (“description”) based on the criteria for a description of a service organization’s system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the Production Inspect Action Platform that may be useful when assessing the risks arising from interactions with METR’s system, particularly information about system controls that METR has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

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

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

- the description presents METR’s Production Inspect Action Platform that was designed and implemented as of August 1, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of August 1, 2025, to provide reasonable assurance that METR’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization applied the complementary controls assumed in the design of METR’s controls as of that date.

Model Evaluation and Threat Research, Inc.
December 16, 2025

SECTION 3:
MODEL EVALUATION AND THREAT RESEARCH, INC.’S DESCRIPTION OF ITS PRODUCTION INSPECT ACTION PLATFORM

MODEL EVALUATION AND THREAT RESEARCH, INC.'S DESCRIPTION OF ITS PRODUCTION INSPECT ACTION PLATFORM

Company Background

Model Evaluation and Threat Research, Inc. ("METR" or "the company") is a 501(c)(3) nonprofit located at 440 N Barranca Ave #3345, Covina, CA 91723. The organization develops scientific methods to assess catastrophic risks stemming from AI systems' autonomous capabilities and seeks to enable informed decision-making regarding their development.

Description of Services Overview

The Production Inspect Action platform (Developed by UK AISI and exclusively operated internally at METR) contains authenticated API endpoints, Kubernetes-based evaluation runners, data stores (S3 logs, DynamoDB run metadata, Vivaria Postgres), the Middleman model-proxy service, and the web viewer. Supporting CI/CD pipelines, secrets management, and alerting are in scope; developer sandboxes and non-production accounts are not.

METR's evaluation platform provides automated execution of AI model evaluations in secure, sandboxed environments. The platform includes user authentication and role-based access control to different model tiers, comprehensive data management for evaluation inputs and results, and full audit logging. The API services enable evaluation submission, monitoring, and result retrieval while integrating with major AI providers. The infrastructure, hosted largely on AWS, provides scalable compute resources, data storage, and automated backup capabilities. All evaluation results are processed through the scoring and reporting system to deliver comprehensive model capability assessments.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

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.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The system description is composed of the following components:

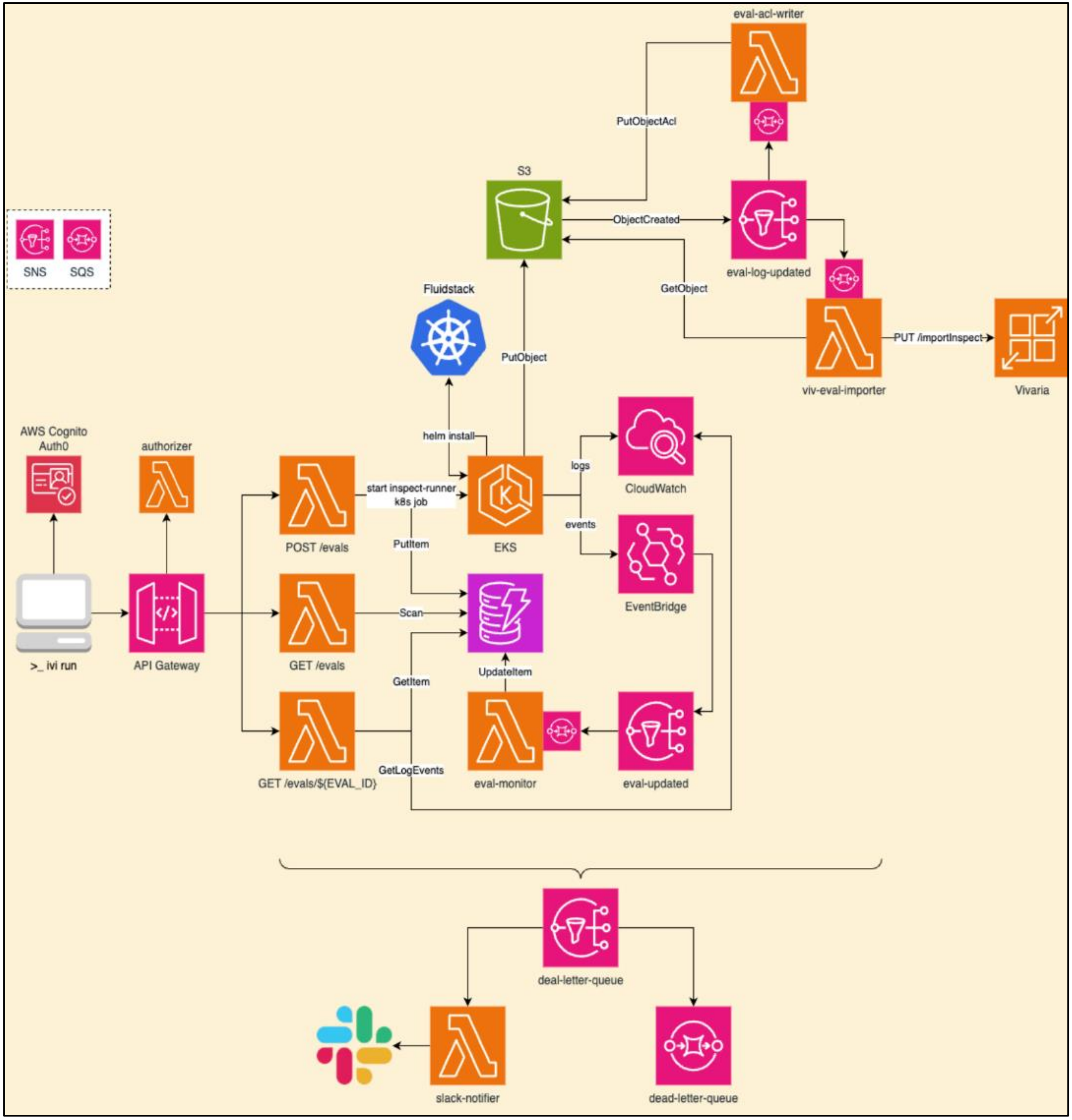
- **Infrastructure** – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.
- **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.

INFRASTRUCTURE

METR maintains a system inventory that includes virtual machines (EC2 instances), and computers (desktops and laptops). The inventory documents device name, device type, vendor function, OS, location, and notes. METR utilizes AWS as a subservice organization to host METR's Production Inspect Action Platform. METR leverages the experience and resources of AWS to enable METR to achieve its service commitments and system requirements. AWS is responsible for designing and configuring the METR processing system architecture within AWS to help ensure service commitments and system requirements are met. The in-scope infrastructure components are shown in the table below:

Primary Infrastructure		
Asset	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	AWS	Compute resources for hosting
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
S3 Buckets	AWS	Storage, upload and download
AWS EKS	AWS	Managed Kubernetes
AWS Lambda	AWS	Serverless functions
AWS API Gateway	AWS	Network infrastructure
AWS DynamoDB	AWS	Database
AWS EventBridge	AWS	Event bus service
AWS IAM	AWS	Permission Management
AWS CloudWatch	AWS	Logging
AWS ECR	AWS	Container image registry for internal services
Opentofu	Software	Infrastructure-as-code

To outline the topology of its network, the organization maintains the following network diagram:



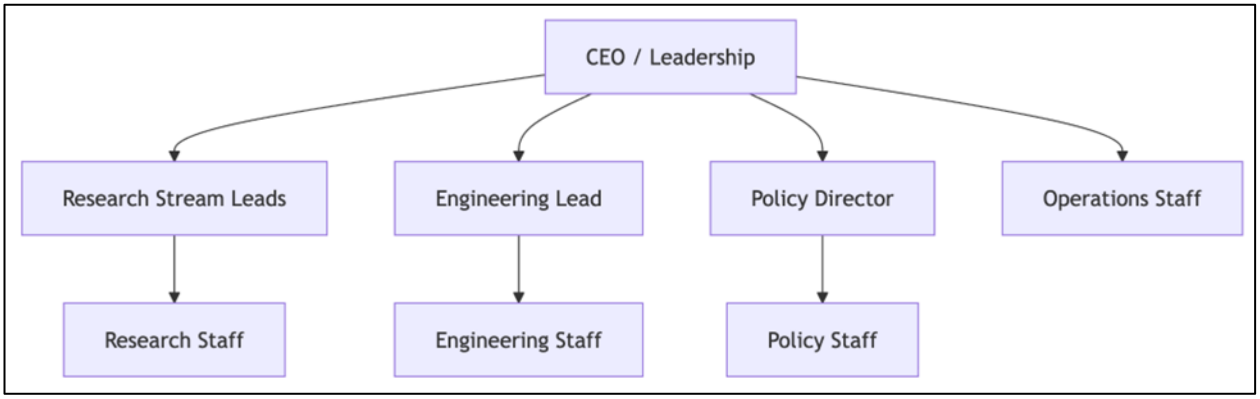
SOFTWARE

The software component consists of the applications, programs, and other software that support the system. The list of software used to build, support, secure, maintain, and monitor the company's Production Inspect Action Platform.

Primary Software	
System/Application	**Purpose**
Datadog	Monitoring application used to provide monitoring, alert, and notification services for Model Evaluation and Threat Research, Inc. platform
AWS	Compute resources for hosting
Auth0	Identity and access management
Checkr	Background checks
GitHub	Source code management
Google Workspace	Email and productivity suite
Kandji	Device management
OpenAI	AI tool
Slack	Internal communications
Vanta	Compliance platform
Bitwarden	Password management
Hugging Face	AI model and dataset access

PEOPLE

The company employs dedicated team members to handle major product functions, including operations and support. The IT/Engineering Team monitors the environment and manages data backups and recovery. The company focuses on hiring qualified personnel for specific roles as well as training them on their tasks and security practices. METR has a staff of approximately 30 staff members organized in the following functional areas:



- **CEO and Leadership:** who has overall responsibility and primarily oversees research.
- **Research Stream Lead:** Leads a research team focused on understanding catastrophic risk from AI models, directing research projects, publishing findings, and building team capabilities to improve METR's risk assessments.
- **Research Staff:** Conducts frontier ML research to assess AI model capabilities and risks, combining research science, execution, and software engineering skills to produce high-quality evaluations and publications.
- **Engineering Lead:** Manages METR's internal platform for evaluating model capabilities, oversees the engineering team, and collaborates with researchers to develop tooling that enables scalable AI evaluations.
- **Engineering Staff:** Builds and maintains infrastructure for running AI agent evaluations at scale, developing tooling that keeps pace with evolving model capabilities and supports researcher workflows.

- **Policy Staff:** Supports policy initiatives including frontier safety policy development, lab partnerships, and government engagement through project management, stakeholder communications, and executive support functions.
- **Operations Lead:** Oversees finance, HR, legal, and governance functions, managing relationships with external counsel and accountants while building scalable operational processes to support organizational growth.
- **Operations Staff:** Provides administrative support across leadership and operations teams, managing logistics, coordinating organizational projects, and executing operational initiatives.

DATA

Data, as defined by METR, is as follows:

User and account data: This includes Personally Identifiable Information (PII) and other information from employees and contractors. Access to PII is controlled through processes for granting system permissions to ensure that PII is restricted to employees based on job function.

METR pays particular attention to confidential data, such as information obtained through privileged access from research partners, and has robust RBAC and monitoring protocols in place to protect it.

METR categorizes data into the following major types:

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for METR.	• Press releases • Public website
Internal	Access to internal information is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Company data	Information collected and used by the company to operate the business. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries
Collaborator data (sensitive)	Sensitive information collected from external collaborators is protected at least as much as company data. Code names, information silos within teams, short data retention, and client-side encryption are examples of methods that have been used to protect such data. METR also enforces mandatory confidentiality training for all employees to ensure the confidentiality policy is closely adhered to.	• Sensitive information from research and policy partners • The performance, identity, or existence or prerelease models

PROCEDURES

METR has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are made annually and authorized by management, the executive team, and control owners.

Physical Security

METR's servers are maintained by AWS, which is responsible for physical security. METR reviews attestation reports and performs a risk analysis of AWS at least annually. Additionally, any destruction of physical assets hosting the production environment is handled by AWS as part of its responsibilities as a subservice provider.

Logical Access

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

Access to these systems is divided into admin roles, user roles, no-access roles, SysAdmin, and BillingAdmin. User access and roles are reviewed quarterly to ensure least-privilege access.

Operations and the System Administrator are responsible for provisioning access to the system based on the employee's role. The employee is responsible for reviewing METR's policies and completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Operations is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination. All devices are fully wiped before reprovisioning or disposal.

Change Management

METR 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, automated continuous deployment, and required approval steps.

Opentofu through GitHub 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 or delegates authority for such approvals separately among others responsible for portions to the production environment. Changes can only be approved by individuals separate from those making the change. Once approved, the change is automatically deployed and leaves a permanent record of the change in the git version control log.

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

Patch Management

Software patches and updates are applied to systems in a timely manner. Infrastructure supporting the services provided is patched as a part of the change management process to help ensure that servers supporting the service are hardened against security threats. Routine updates are applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within three days from identification and non-critical security patches are applied within seven days after identification.

Computer Operations

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

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

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

Problem Management

METR maintains an Incident Response Policy that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined.

Data Communications

METR 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 the logical network configuration by providing an effective firewall around all METR application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints which are themselves only accessible when authorized users are connected to METR's tailscale VPN.

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

METR uses a monitoring service across its key platforms to detect any unusual activity and consults with security firms to identify vulnerabilities.

System Monitoring

The Network Security and Vulnerability Management Policy describes the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses DataDog for system logging within the AWS SSO environment and across other platforms. DataDog logs document source IP, destination IP, username, and timestamp. The organization monitors system capacity using DataDog.

DataDog, Kandji, and Santa are used for threat detection purposes, and the tools generate logs, including for intrusion detection.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses Santa and Kandji to protect against malware and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year with at least three months readily available. This software is used to identify newly emerging vulnerabilities, and the organization monitors vendors, for patch updates to correct vulnerabilities.

Vendor Management

The organization maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendors' cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

Boundaries of the System

The boundaries of the Production Inspect Action Platform include the specific aspects of METR's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services delivered. Any infrastructure, software, people, procedures, and data that indirectly support these services are not included within the boundaries of the Production Inspect Action Platform.

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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, CONTROL ACTIVITIES, INFORMATION AND COMMUNICATION, AND MONITORING CONTROLS

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by department and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement, and ensure effective operational controls. The Board of Directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

Integrity and Ethical Values

The effectiveness of controls cannot exceed the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of METR's control environment, influencing the design, administration, and monitoring of other components. Integrity and ethical behavior stem from METR'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 organizational values and behavioral standards to personnel through policy statements and codes of conduct.

Specific control activities implemented in this area are described below:

- Formally documented organizational policy statements and codes of conduct communicate values and behavioral standards to personnel.
- Policies and procedures require employees to 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 signed confidentiality agreement agreeing not to disclose proprietary or confidential information, including external parties, to unauthorized parties is a component of the employee code of conduct.
- Background checks are performed for employees as part of the hiring process.

Management Philosophy and Operating Style

The METR management team must balance two competing interests: continuing to grow and innovate in a cutting-edge, rapidly changing technology space while remaining excellent and careful stewards of the sensitive data and workflows entrusted to the organization.

Specific control activities implemented in this area are described below:

- Management periodically discusses regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.
- The organization’s Board of Directors is ultimately responsible for the oversight of cyber-risk and internal control for information security, privacy and compliance. They are also responsible for consulting with executive leadership when needed to understand the organization’s IT mission and risks and providing guidance to align business, IT, and security objectives.

Commitment to Competence

METR'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 consideration of the competence levels required for jobs and how those levels translate into the requisite skills and knowledge.

The specific control activity implemented in this area is described below:

- Training may be provided to maintain the skill level of personnel in certain positions.
- A large professional development budget supports knowledge and skill growth.
- Hiring involves looking for excellent track records and/or strong performance or rigorous and realistic work tests.

Organizational Structure and Assignment of Authority and Responsibilities

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

METR's assignment of authority and responsibility 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, the knowledge and experience of key personnel, and the resources provided for carrying out duties. In addition, it includes policies and communications aimed 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.

The specific control activity implemented in this area is described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Expense approval policies, approvals archiving, and other internal infrastructure communicates specific areas of responsibility.

Human Resources Policies and Procedures

METR's success is founded on sound business ethics, reinforced by a high level of efficiency, integrity, and ethical standards. This success is evidenced by its proven track record of hiring and retaining top-quality personnel who ensure the organization operates at maximum efficiency. METR's human resources policies and practices cover employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee code of conduct and a confidentiality upon joining.
- Evaluations for each employee are performed at least on an annual basis.
- Personnel termination procedures are documented in a termination checklist to guide the process.

RISK ASSESSMENT PROCESS

METR's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable and secure services to partners. As part of this process, METR 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 METR's product development process to ensure they are addressed predictably and iteratively.

Integration with Risk Assessment

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

CONTROL ACTIVITIES

Control activities are actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and at various stages within business processes and across the technology environment.

INFORMATION AND COMMUNICATION SYSTEM

Information and communication are integral components of METR's internal control system. They involve identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the entity's operations.

METR uses several internal communication channels to share information with management and employees, including chat systems and email as the primary internal and external communication tools.

MONITORING CONTROLS

Management monitors controls to ensure they operate as intended and are modified as conditions change. METR's management performs monitoring activities to continuously assess the quality of internal control over time. Corrective actions are taken as needed to address deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored through ongoing monitoring activities, separate evaluations, or a combination of both.

Ongoing Monitoring

METR's management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective actions through team meetings, internal conference calls, and informal notifications.

Management's close involvement in METR's operations helps identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. Decisions for addressing control weaknesses are based on whether the incident was isolated or requires changes to company procedures or personnel. The goal of this process is to ensure legal compliance and maximize personnel performance.

Monitoring of the Subservice Organization

METR uses AWS to provide hosting services.

METR's management receives and reviews AWS's SOC 2 report annually (or delegates this task). In addition, through daily operational activities, METR monitors AWS's services to ensure that operations and controls expected to be implemented at AWS are functioning effectively.

Reporting Deficiencies

The organization's internal risk management tracking tool is used to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding to and notifying management of identified risks, and instructions for escalation are provided to employees in company policy documents. Risks receiving a high rating are addressed 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.

CHANGES TO THE SYSTEM AFTER THE EXAMINATION DATE

Transitioning from Vivaria to Inspect Action: the primary internal service used/actively developed for has changed to inspect-action, which is based on the open-source project inspect, a framework for large language model evaluations created by the UK AI Security Institute.

SYSTEM INCIDENTS AFTER THE EXAMINATION DATE

No significant incidents have occurred to the services provided to user entities since the point in time date of this report.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

METR's controls related to the system cover only a portion of overall internal control for each user entity of METR. It is not feasible for the trust services criteria related to the system to be achieved solely by METR. Therefore, each user entity's internal controls should be evaluated in conjunction with METR's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	AWS is responsible for maintaining physical security over the data centers hosting the METR infrastructure.	CC6.4
2	AWS is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

The METR's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

SECTION 4:
TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

Trust Services Category, Criteria, and Related Controls

This SOC 2 Type 1 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* throughout the period August 1, 2025.

The applicable trust services criteria and related controls specified by METR are presented in Section 4 of this report.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ENVIRONMENT	
Control Number	Controls
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	The company performs background checks on new employees.
CC1.1.2	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.
CC1.1.3	The company requires contractors to sign a confidentiality agreement at the time of engagement.
CC1.1.4	The company requires employees to sign a confidentiality agreement during onboarding.
CC1.1.5	The company managers are required to complete performance evaluations for direct reports at least annually.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	The company's board of directors is briefed by 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.
CC1.2.2	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.
CC1.2.3	The board includes directors that are independent of the company.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	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.
CC1.3.2	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
CC1.3.3	The company maintains an organizational chart that describes the organizational structure and reporting lines.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	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.
CC1.4.2	The company performs background checks on new employees.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ENVIRONMENT	
Control Number	**Controls**
CC1.4.3	The company managers are required to complete performance evaluations for direct reports at least annually.
CC1.4.4	The company requires employees to complete security awareness training within thirty days of hire and at least annually.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	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.
CC1.5.2	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.
CC1.5.3	The company managers are required to complete performance evaluations for direct reports at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
COMMUNICATION AND INFORMATION	
Control Number	Controls
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.
CC2.1.2	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.
CC2.1.3	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	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.
CC2.2.2	The company communicates system changes to authorized internal users via intranet/communication channel.
CC2.2.3	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.
CC2.2.5	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.
CC2.2.6	The company provides a description of its products and services to internal and external users.
CC2.2.7	The company requires employees to complete security awareness training within thirty days of hire and at least annually.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	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.
CC2.3.2	The company notifies customers of critical system changes that may affect their processing via web site.
CC2.3.3	The company's security commitments are required to be communicated to customers via written agreements.
CC2.3.4	The company provides guidelines and technical support resources relating to system operations to customers.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
COMMUNICATION AND INFORMATION	
Control Number	Controls
CC2.3.5	The company provides a description of its products and services to internal and external users.
CC2.3.6	The company has written agreements in place with vendors and related third-parties. These agreements include security commitments applicable to that entity.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
RISK ASSESSMENT	
Control Number	**Controls**
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.
CC3.1.2	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC3.1.3	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.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	The company has a documented business continuity/disaster recovery (BC/DR) plan and requires to test the business continuity/disaster recovery (BC/DR) plan at least annually.
CC3.2.2	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.
CC3.2.3	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.
CC3.2.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	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.
CC3.3.2	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
RISK ASSESSMENT	
Control Number	**Controls**
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	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.
CC3.4.2	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.
CC3.4.3	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.
CC3.4.4	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
MONITORING ACTIVITIES	
Control Number	**Controls**
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.
CC4.1.2	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.
CC4.1.3	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.
CC4.1.4	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.
CC4.2.2	The company's security 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.
CC4.2.3	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.
CC4.2.4	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ACTIVITIES	
Control Number	**Controls**
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	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.
CC5.1.2	The company’s information security policies and procedures are documented and reviewed at least annually.
CC5.1.3	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.
CC5.1.4	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.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	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.
CC5.2.2	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.
CC5.2.3	The company’s information security policies and procedures are documented and reviewed at least annually.
CC5.2.4	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.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	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.
CC5.3.2	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ACTIVITIES	
Control Number	**Controls**
CC5.3.3	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.
CC5.3.4	The company’s information security policies and procedures are documented and reviewed at least annually.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC5.3.6	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.
CC5.3.7	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.

<table>
<tr><th colspan="2">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="2">LOGICAL AND PHYSICAL ACCESS CONTROLS</th></tr>
<tr><th>Control Number</th><th>Controls</th></tr>
<tr><td colspan="2"><b>CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</b></td></tr>
<tr><td>CC6.1.1</td><td>The company maintains a formal inventory of production system assets.</td></tr>
<tr><td>CC6.1.2</td><td>The company's datastores housing sensitive customer data are encrypted at rest.</td></tr>
<tr><td>CC6.1.3</td><td>The company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.</td></tr>
<tr><td>CC6.1.4</td><td>The company restricts administrative access to system components to only authorized personnel (network, networking devices, database, operating system, application, encryption keys, moving changes to production).</td></tr>
<tr><td>CC6.1.5</td><td>System access restricted to authorized access only.</td></tr>
<tr><td>CC6.1.6</td><td>The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.</td></tr>
<tr><td>CC6.1.7</td><td>The company requires passwords for in-scope system components to be configured according to the company's policy.</td></tr>
<tr><td>CC6.1.8</td><td>The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.</td></tr>
<tr><td>CC6.1.9</td><td>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.</td></tr>
<tr><td>CC6.1.10</td><td>The company ensures that user access to in-scope system components is based on job role and function.</td></tr>
<tr><td>CC6.1.11</td><td>The company's network is segmented to prevent unauthorized access to customer data.</td></tr>
<tr><td colspan="2"><b>CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</b></td></tr>
<tr><td>CC6.2.1</td><td>The company conducts access reviews on a quarterly basis for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.</td></tr>
<tr><td>CC6.2.2</td><td>The company requires authentication methods to in-scope systems to include a unique username, password, MFA, and/or SSH keys.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	Controls
CC6.2.3	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.
CC6.2.4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
CC6.2.5	The company ensures that user access to in-scope system components is based on job role and function.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	The company conducts access reviews on a quarterly basis for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.3.2	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.
CC6.3.3	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
CC6.3.4	The company ensures that user access to in-scope system components is based on job role and function.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
Management contracts with AWS to provide physical access security of its production systems; therefore, this criterion is the responsibility of the subservice organization.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.5.1	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.
CC6.5.2	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company data.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Controls**
CC6.5.3	The company requires to purge or remove customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.
CC6.5.4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
The destruction of physical assets hosting the production environment is the responsibility of AWS; therefore, part of this criterion is the responsibility of the subservice organization.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.6.2	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
CC6.6.3	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
CC6.6.4	The company reviews its firewall rule sets at least annually. Required changes are tracked to completion.
CC6.6.5	The company uses firewalls and configures them to prevent unauthorized access.
CC6.6.6	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
CC6.6.7	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.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7.1	The company encrypts portable devices when used.
CC6.7.2	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.
CC6.7.3	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Controls**
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC6.8.1	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.
CC6.8.2	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.
CC6.8.3	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.
CC6.8.4	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
SYSTEM OPERATIONS	
Control Number	Controls
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
CC7.1.1	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
CC7.1.2	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.
CC7.1.3	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.
CC7.1.4	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.1.5	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.
CC7.1.6	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.2.1	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
CC7.2.2	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.
CC7.2.3	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
SYSTEM OPERATIONS	
Control Number	**Controls**
CC7.2.4	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2.5	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.
CC7.2.6	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.
CC7.3.2	The company's security 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.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
CC7.4.1	The company tests its Incident Response Plan at least annually.
CC7.4.2	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.
CC7.4.3	The company's security 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.
CC7.4.4	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.
CC7.4.5	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	The company has a documented business continuity/disaster recovery (BC/DR) plan and requires to test the business continuity/disaster recovery (BC/DR) plan at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
SYSTEM OPERATIONS	
Control Number	Controls
CC7.5.2	The company tests its Incident Response Plan at least annually.
CC7.5.3	The company has security incident response policies and procedures that are documented and communicated to authorized users via the compliance platform.
CC7.5.4	The company's security 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CHANGE MANAGEMENT	
Control Number	**Controls**
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CC8.1.1	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.
CC8.1.2	The company restricts access to migrate changes to production to authorized personnel.
CC8.1.3	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.
CC8.1.4	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
CC8.1.5	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.
CC8.1.6	Host-based vulnerability scans/external-facing assets are performed continuously on all in-scope systems. Critical and high vulnerabilities are tracked to remediation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
RISK MITIGATION	
Control Number	**Controls**
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	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.
CC9.1.2	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.
CC9.1.3	The company tests its Incident Response Plan at least annually.
CC9.1.4	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.
CC9.1.5	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.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	The company has written agreements in place with vendors and related third-parties. These agreements include security commitments applicable to that entity.
CC9.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.