SYSTEM AND ORGANIZATION CONTROLS (SOC) 2 TYPE 2
REPORT ON MANAGEMENT'S DESCRIPTION OF ITS

Software as a Service System

And the Suitability of Design of Controls Relevant to the Controls Placed in Operation and Test of Operating Effectiveness Relevant to: Trust Services Criteria for Security, Availability, and Confidentiality

For the period 19 June 2025 to 18 September 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report 1

Scope 1

Service Organization's Responsibilities 1

Service Auditors' Responsibilities 2

Inherent Limitations 3

Description of Tests of Controls 3

Opinion 3

Restricted Use 4

2. Assertion of Exa Management 5

3. Description of Exa's Software as a Service System 7

Company Background 7

Services Provided 7

Principal Service Commitments and System Requirements 7

Components of the System 8

4. Description of Criteria, Controls, Tests and Results of Tests ... 17

1. Independent Service Auditors' Report

To the Management of Exa Labs Inc. (Exa)

Scope

We have examined Exa's accompanying description of its Software as a Service System titled "Description of Exa's Software as a Service System" (description) throughout the period 19 June 2025 to 18 September 2025, 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 and operating effectiveness of controls stated in the description throughout the period 19 June 2025 to 18 September 2025, to provide reasonable assurance that Exa's service commitments and system requirements were achieved based on:

- the Trust Services Criteria relevant to Security, Availability, and Confidentiality (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*.

Exa uses subservice organizations to provide computing, storage, processing and other services to support their system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Exa, to achieve Exa's service commitments and system requirements based on the applicable trust services criteria. The description presents Exa's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Exa's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Exa 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 Exa's service commitments and system requirements were achieved. Exa has

provided the accompanying assertion titled “Assertion of Exa Management” (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Exa 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 Auditors’ Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the 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 operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects,

a. the description presents Exa's Software as a Service System that was designed and implemented throughout the period 19 June 2025 to 18 September 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period 19 June 2025 to 18 September 2025, to provide reasonable assurance that Exa's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Exa's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period 19 June 2025 to 18 September 2025 to provide reasonable assurance that Exa's service commitments and system requirements were achieved based on the applicable trust services criteria, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Exa's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section 4, is intended solely for the information and use of Exa, user entities of Exa's Software as a Service System during some or all of the period 19 June 2025 to 18 September 2025, business partners of Exa subject to risks arising from interactions with the Software as a Service System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Sensiba LLP

San Jose, California
22 October 2025

2. Assertion of Exa Management

We have prepared the accompanying description of Exa Labs Inc.'s (Exa) Software as a Service System titled "*Description of Exa's Software as a Service System*" (description) throughout the period 19 June 2025 to 18 September 2025, 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 Software as a Service System that may be useful when assessing the risks arising from interactions with Exa's system, particularly information about system controls that Exa has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on:

- the Trust Services Criteria relevant to Security, Availability, and Confidentiality (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*.

Exa uses subservice organizations to provide computing, storage, processing and other services to support their system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Exa, to achieve Exa's service commitments and system requirements based on the applicable trust services criteria. The description presents Exa's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Exa's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents Exa's Software as a Service System that was designed and implemented throughout the period 19 June 2025 to 18 September 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period 19 June 2025 to 18 September 2025, to provide reasonable assurance that Exa's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the

subservice organization and user entities applied the complementary controls assumed in the design of Exa's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period 19 June 2025 to 18 September 2025 to provide reasonable assurance that Exa's service commitments and system requirements were achieved based on the applicable trust services criteria, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Exa's controls operated effectively throughout that period.

Signed by Exa Management

22 October 2025

3. Description of Exa's Software as a Service System

Company Background

Exa is an AI-native web search platform built from the ground up for LLMs, agents, and AI-first products. Unlike typical search APIs that wrap existing engines, Exa owns the full stack—crawl, index, ranking, verification— to get full control, transparency, and performance.

Exa's mission: perfect web search for AI.

Services Provided

Exa provides a suite of powerful endpoints designed to meet the evolving needs of AI systems:

- Contents – Retrieve complete, cleaned webpage content in a single API call. Ideal for RAG pipelines, dataset creation, and content analysis.
- Search – Access high-quality, ranked web results with optional full content in under one
- second
- Research – Conduct multi-step, autonomous investigations across thousands of sources, returning structured, factual summaries.
- Websets – Build structured datasets of verified entities that meet user-defined criteria. Websets leverage an agentic workflow to validate and enrich each result, returning thousands of accurate matches.

Principal Service Commitments and System Requirements

Exa has established processes, policies, and procedures to meet its objectives related to its Software as a Service System (the 'System'). Those objectives are based on the purpose, vision, and values of Exa as well as commitments that Exa makes to user entities, the requirements of laws and regulations that apply to Exa's activities, and the operational requirements that Exa has established.

Commitments are documented, and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in Exa's processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

Components of the System

Infrastructure
Exa's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of AWS.

System	Type	Description
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	Secure and resizable compute capacity (virtual servers) in the cloud.
Amazon Elastic Container Service (ECS)	Cloud Compute	Secure, reliable, and scalable service to run containers.
Amazon Elastic Kubernetes Service (EKS)	Cloud Compute	Fully managed Kubernetes service.
AWS Lambda	Cloud Compute	Serverless, event-driven compute service.
PostgreSQL	Data Storage	Open-source relational database management system emphasizing extensibility and SQL compliance.
Amazon RDS	Data Storage	Relational database service.
Amazon DynamoDB	Data Storage	Key value database service.
Amazon Simple Storage Service (S3)	Data Storage	Object, file, and block storage.
Cloudflare	Network Services	DNS, load balancing, DDOS protection, web firewall and TLS encryption.
AWS Elastic Load Balancing (ELB)	Networking	Automatically distributes incoming application traffic across multiple targets.
AWS Key Management Service	Key Management	Centralized control over the cryptographic keys used to protect data.

Software
Primary software is used to support Exa's system.

Software	Purpose
Exa API Websets	The Software as a Service System provided to Exa customers.

Software	Purpose
AWS CloudTrail	Enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage on AWS.
AWS CloudWatch	Monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources.
AWS GuardDuty	Threat detection service that continuously monitors AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.
AWS Inspector	Automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
GitHub	Source code repository used to manage the software code and version control.
GitHub Actions	Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment.
GitHub Dependabot	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
1Password	Enterprise password manager used to store authentication secrets and strengthen password security.
Prometheus	System monitoring software used to log events and raise alerts to support system security and availability.
Linear	Ticketing software used to log events and requirements to support the internal controls.
Gusto, Deel	Human resources information system used to manage employee processes like onboarding, offboarding and performance.
Google Workspace	Google's suite of enterprise productivity, collaboration, and communication tools.
Vanta	Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance.

People

Exa's personnel are organized into the following functional areas:

- Leadership: The executive level responsible for corporate governance.
- Engineering: Responsible for building and maintaining the infrastructure and software.
- Customer Success: Responsible for the customer experience, support, and services.
- Sales: Responsible for onboarding new customers and aligning requirements.

- Marketing: Responsible for branding, market positioning and attracting customers.

Data
The data collected and processed by Exa includes the following types:

- Basic personal details: name, email, contact details.
- User activity: user activity within the software.
- Financial account information: account balances, transactions.
- Payment information: credit card information.

Processes, Policies and Procedures
Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with Exa's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Exa's employees and can be referred to as needed.

Compliance Management Platform
Exa uses compliance automation software, Vanta, to support the design, implementation, operation, monitoring, and documentation of internal controls. Vanta leverages APIs to centralize the monitoring of Exa's information assets across their infrastructure provider, identity manager, code repository, and endpoint devices. These APIs in combination with compliance automation functions in Vanta support the continuous monitoring of control activities for Exa's people, devices, policies, procedures and plans, risk assessments, third-party vendor assessments, system monitoring and the security configurations of these critical systems.

Using Vanta does not reduce management's responsibility for designing, implementing, and operating an effective system of internal control. Exa evaluates the accuracy and completeness of the information stored in Vanta and conducts annual vendor risk assessments.

Physical Security
The critical infrastructure and data of the System are hosted by AWS. There are no trusted local office networks. As such, AWS is responsible for the key physical security controls that support the System.

Logical Access
Exa's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfil job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are periodically reviewed and adjusted when no longer required. Additional information security policies and procedures require Exa employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, periodic testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Exa employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data.

System Operations
Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Exa's critical infrastructure and data are hosted by AWS to provide failover capability in the event of an outage of one of the data centers. Redundancy, disaster recovery in continuity considerations are built into the system design of AWS to support Exa's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control
Exa operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the Exa API Websets software to support Exa's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub version control software is used for the code repository that tracks all changes to the Exa API Websets software, including managing versions and roll-back capability in the event of a failed change release.

A continuous integration / continuous deployment (CI/CD) pipeline is configured using GitHub Actions to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment. Changes to the infrastructure configurations and settings are managed as code, subject to the same process steps and checks prior to impacting the production environment.

Data Governance
Exa uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of Exa.

Established processes, policies, procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Control Environment
Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Exa's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Exa's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those 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.

Commitment to Competence

Exa's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Exa's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams and the company as a whole.

Management's Philosophy and Operating Style

Exa's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Exa's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

Exa's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Exa's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Human Resource Policies and Practices

Exa's employees are the foundation for achieving the objectives and commitments. Exa's hiring, onboarding and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation, and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Risk Assessment Process

Exa's risk assessment process identifies and manages risks that threaten achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Exa, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Exa's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance risk – legal and regulatory obligations and changes.
- Financial risk – the sustainability of Exa and resources supporting the objectives.

These risks are identified by Exa management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in Exa's context.

Integration with Risk Assessment

Established internal controls include Exa's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the

changing landscape and requirement of those controls as Exa grows, and the associated risks change.

Information and Communications Systems

Information and communication are a core part of Exa'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 Exa's operations effectively. The information and communication systems consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, regulators, and shareholders.
The information and communication systems include central tracking systems that support Exa's established processes, as well as various meetings, and documented policies, procedures, and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers Exa's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the board, for ensuring appropriate actions are completed in a timely manner.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Criteria Not Applicable to the System

All Security, Availability, and Confidentiality Trust Services Criteria were applicable to Exa's Software as a Service System.

Subservice Organizations
This report does not include the cloud hosting services provided by AWS.

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Security	CC6.1-CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
Security	CC6.4	Policies and procedures are established and followed to restrict physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers.
Security	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
Security	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.
Availability	A1.2	Procedures are established and followed to manage environmental protections within the data centers that house network, virtualization management, and storage devices supporting cloud hosting services where the system resides.

Exa management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, Exa performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

Complementary User Entity Controls

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

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Agreed 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 Exa's terms of service.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Ensuring multi-factor authentication is applied by personnel, if required.
- Performing any required risk assessments and approvals when using pre-built integrations available with Exa's services.
- Ensuring the supervision, management, and control of the use of Exa's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Exa services for any critical reliance on these services.

4. Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and Exa related controls are an integral part of management's system description and are included in this section. Sensiba LLP performed testing to determine if Exa's controls were suitably designed and operating effectively to achieve the specified criteria for Security, Availability, and Confidentiality 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 19 June 2025 to 18 September 2025.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Exa activities and operations and inspection of Exa documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Exa controls, this test was not listed individually for every control in the tables below.

Common Criteria 1: Control Environment

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The information security policies are communicated, read and acknowledged by employees.	Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees.	No exceptions noted
		Background checks are conducted for new hires.	Inspected the background checks for a sample of new hires to determine that background checks were conducted for new hires.	No exceptions noted
		Exa evaluates the performance of all employees through a formal, annual performance review.	Inspected the performance reviews for a sample of employees to determine that Exa evaluated the performance of all employees through a formal, annual performance review.	No exceptions noted
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.	Inspected the code of conduct to determine that Exa established workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.	No exceptions noted
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Exa's board of directors has a documented charter that outlines the roles, responsibilities, and key activities of the board.	Inspected the board charter to determine that Exa's board of directors had a documented charter that outlined the roles, responsibilities, and key activities of the board.	No exceptions noted
		Exa's board of directors meets at least annually and maintains meeting minutes.	Inspected the board meeting minutes to determine that Exa's board of directors met at least annually and maintained meeting minutes.	No exceptions noted
		The documented organization chart outlines the roles, functional responsibilities and reporting lines for Exa personnel and demonstrates independence between management and the board of directors.	Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Exa personnel and demonstrates independence between management and the board of directors.	No exceptions noted

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The documented organization chart outlines the roles, functional responsibilities and reporting lines for Exa personnel and demonstrates independence between management and the board of directors.	Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Exa personnel and demonstrates independence between management and the board of directors.	No exceptions noted
		Exa's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	Inspected the information security policies to determine that Exa's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	No exceptions noted
		Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the defined roles and responsibilities to determine that management had established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	No exceptions noted
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and	Security awareness training is conducted for Exa employees at least annually.	Inspected the records of security awareness training to determine that security awareness training was conducted for Exa employees at least annually.	No exceptions noted

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	retain competent individuals in alignment with objectives.	Background checks are conducted for new hires.	Inspected the background checks for a sample of new hires to determine that background checks were conducted for new hires.	No exceptions noted
		Exa evaluates the performance of all employees through a formal, annual performance review.	Inspected the performance reviews for a sample of employees to determine that Exa evaluated the performance of all employees through a formal, annual performance review.	No exceptions noted
		Exa establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.	Inspected the code of conduct to determine that Exa established workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.	No exceptions noted
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control	Exa evaluates the performance of all employees through a formal, annual performance review.	Inspected the performance reviews for a sample of employees to determine that Exa evaluated the performance of all employees through a formal, annual performance review.	No exceptions noted

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	responsibilities in the pursuit of objectives.	The documented organization chart outlines the roles, functional responsibilities and reporting lines for Exa personnel and demonstrates independence between management and the board of directors.	Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Exa personnel and demonstrates independence between management and the board of directors.	No exceptions noted
		Exa's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	Inspected the information security policies to determine that Exa's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	No exceptions noted
		Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the defined roles and responsibilities to determine that management had established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	No exceptions noted

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted
		Exa establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.	Inspected the code of conduct to determine that Exa established workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.	No exceptions noted

Common Criteria 2: Information and Communication

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Exa maintains an architecture diagram to document the system boundaries and support the functioning of internal control.	Inspected the architecture diagram to determine that Exa maintained an architecture diagram to document the system boundaries and support the functioning of internal control.	No exceptions noted
		Information logs related to the information processing activities are centrally stored for retrospective analysis where required.	Inspected the configuration of log capture to determine that information logs related to the information processing activities were centrally stored for retrospective analysis where required.	No exceptions noted
		Exa conducts continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	Inspected the continuous monitoring in Vanta to determine that Exa conducted continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	No exceptions noted
		The information assets are identified, classified, and centrally tracked in Vanta for ongoing monitoring and governance.	Inspected the information asset register to determine that the information assets were identified, classified, and centrally logged in Vanta for ongoing monitoring and governance.	No exceptions noted
		Exa has an established policy and procedures that governs the use of cryptographic controls.	Inspected the encryption policy to determine that Exa had an established policy and procedures that governed the use of cryptographic controls.	No exceptions noted

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed.	Inspected the secure disposal policies and procedures to determine that the disposal of sensitive information assets followed a defined process to ensure sensitive data was effectively erased before the safeguards over the information assets were removed.	No exceptions noted
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Exa conducts continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	Inspected the continuous monitoring in Vanta to determine that Exa conducted continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	No exceptions noted
		The information security policies are communicated, read and acknowledged by employees.	Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees.	No exceptions noted
		Security awareness training is conducted for Exa employees at least annually.	Inspected the records of security awareness training to determine that security awareness training was conducted for Exa employees at least annually.	No exceptions noted

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	Inspected the information security policies to determine that Exa's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	No exceptions noted
		Exa defines the contacts and methods for employees to report security-related incidents and concerns.	Inspected the responsible disclosure policy to determine that Exa defined the contacts and methods for employees to report security-related incidents and concerns.	No exceptions noted
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Exa follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident handling for a sample of incidents to determine that Exa followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	No exceptions noted
		Terms of service are agreed with Exa's customers and users of the services to communicate their responsibilities and terms of use.	Inspected the terms of service to determine that terms of service were agreed with Exa's customers and users of the services to communicate their responsibilities and terms of use.	No exceptions noted
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.	Inspected the vendor register to determine that the vendor register included material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.	No exceptions noted
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	Inspected the vendor management policy to determine that Exa set out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	No exceptions noted

Common Criteria 3: Risk Assessment

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The information security policies are communicated, read and acknowledged by employees.	Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees.	No exceptions noted
		Exa conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	Inspected the risk assessments to determine that Exa conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	No exceptions noted
		Exa's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	Inspected the risk remediation plan to determine that Exa's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	No exceptions noted
		Exa has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	Inspected the risk assessment policy to determine that Exa had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	No exceptions noted

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	Inspected the risk assessments to determine that Exa conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	No exceptions noted
		Exa's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	Inspected the risk remediation plan to determine that Exa's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	No exceptions noted
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.	Inspected the vendor register to determine that the vendor register included material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.	No exceptions noted
		Exa performs security and compliance assessments of critical and high-risk vendors.	Inspected the security and compliance review for a sample of critical and high-risk vendors to determine that Exa performed security and compliance assessments of high-risk vendors.	No exceptions noted

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	Inspected the risk assessment policy to determine that Exa had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	No exceptions noted
		Exa sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	Inspected the vendor management policy to determine that Exa set out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	No exceptions noted
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Exa conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	Inspected the risk assessments to determine that Exa conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	No exceptions noted
		Exa's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	Inspected the risk remediation plan to determine that Exa's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	No exceptions noted

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	Inspected the risk assessment policy to determine that Exa had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	No exceptions noted
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Exa conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	Inspected the risk assessments to determine that Exa conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	No exceptions noted
		Exa's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	Inspected the risk remediation plan to determine that Exa's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	No exceptions noted
		Exa has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	Inspected the risk assessment policy to determine that Exa had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	No exceptions noted

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	Inspected the vendor management policy to determine that Exa set out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	No exceptions noted

Common Criteria 4: Monitoring Activities

CC4.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa conducts continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	Inspected the continuous monitoring in Vanta to determine that Exa conducted continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	No exceptions noted
		Vanta is used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	Inspected the Vanta monitoring to determine that Vanta was used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	No exceptions noted
		Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted
		Independent penetration tests are conducted annually.	Inspected the penetration test report to determine that independent penetration tests were conducted annually.	No exceptions noted

CC4.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa conducts continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	Inspected the continuous monitoring in Vanta to determine that Exa conducted continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	No exceptions noted
		Vanta is used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	Inspected the Vanta monitoring to determine that Vanta was used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	No exceptions noted
		Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted
		Independent penetration tests are conducted annually.	Inspected the penetration test report to determine that independent penetration tests were conducted annually.	No exceptions noted

CC4.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted

Common Criteria 5: Control Activities

CC5.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa conducts continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	Inspected the continuous monitoring in Vanta to determine that Exa conducted continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	No exceptions noted
		Vanta is used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	Inspected the Vanta monitoring to determine that Vanta was used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	No exceptions noted
		Exa conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	Inspected the risk assessments to determine that Exa conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	No exceptions noted
		Exa's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	Inspected the risk remediation plan to determine that Exa's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	No exceptions noted

CC5.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	Inspected the risk assessment policy to determine that Exa had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	No exceptions noted
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Exa conducts continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	Inspected the continuous monitoring in Vanta to determine that Exa conducted continuous monitoring of the security controls using Vanta with automated alerts and tracking of the control effectiveness over time.	No exceptions noted
		The information security policies are reviewed by management at least annually and updated where required.	Inspected the review of the information security policies to determine that the information security policies were reviewed by management at least annually and updated where required.	No exceptions noted
		The information security policies are communicated, read and acknowledged by employees.	Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees.	No exceptions noted

CC5.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted
		Independent penetration tests are conducted annually.	Inspected the penetration test report to determine that independent penetration tests were conducted annually.	No exceptions noted
		Exa requires appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	Inspected the access control policy to determine that Exa required appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	No exceptions noted
		Exa defines the contacts and methods for employees to report security-related incidents and concerns.	Inspected the responsible disclosure policy to determine that Exa defined the contacts and methods for employees to report security-related incidents and concerns.	No exceptions noted
		Exa has an established policy and procedures that governs the use of cryptographic controls.	Inspected the encryption policy to determine that Exa had an established policy and procedures that governed the use of cryptographic controls.	No exceptions noted

CC5.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	The information security policies are reviewed by management at least annually and updated where required.	Inspected the review of the information security policies to determine that the information security policies were reviewed by management at least annually and updated where required.	No exceptions noted
		The information security policies are communicated, read and acknowledged by employees.	Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees.	No exceptions noted
		Exa's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	Inspected the information security policies to determine that Exa's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.	No exceptions noted

Common Criteria 6: Logical and Physical Access Controls

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa stores sensitive data, including customer data, in databases that are encrypted at rest.	Inspected the database encryption to determine that Exa stored sensitive data, including customer data, in databases that were encrypted at rest.	No exceptions noted
		Multi-factor authentication is required for access to sensitive systems.	Inspected the monitoring of multi-factor authentication to determine that multi-factor authentication was required for access to sensitive systems.	No exceptions noted
		User accounts are individually assigned with a unique user ID to support system logging and accountability.	Inspected the monitoring of unique user ID's to determine that user accounts were individually assigned with a unique user ID to support system logging and accountability.	No exceptions noted
		Exa's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	Inspected the monitoring of hard-disk encryption for devices to determine that Exa's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	No exceptions noted
		The information assets are identified, classified, and centrally tracked in Vanta for ongoing monitoring and governance.	Inspected the information asset register to determine that the information assets were identified, classified, and centrally logged in Vanta for ongoing monitoring and governance.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa requires appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	Inspected the access control policy to determine that Exa required appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	No exceptions noted
		Exa has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the password policy to determine that Exa had established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and	User accounts are individually assigned with a unique user ID to support system logging and accountability.	Inspected the monitoring of unique user ID's to determine that user accounts were individually assigned with a unique user ID to support system logging and accountability.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	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.	New hires and other new system access requirements are approved as part of the onboarding process or by authorized system owners prior to access being granted.	Inspected the access approval for a sample of new hires to determine that new hires and other new system access requirements were approved as part of the onboarding process or by authorized system owners prior to access being granted.	No exceptions noted
		A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner.	No exceptions noted.
		Quarterly reviews of Exa's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required.	Inspected the user access review for a sample of quarters to determine that quarterly reviews of Exa's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa requires appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	Inspected the access control policy to determine that Exa required appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and	User accounts are individually assigned with a unique user ID to support system logging and accountability.	Inspected the monitoring of unique user ID's to determine that user accounts were individually assigned with a unique user ID to support system logging and accountability.	No exceptions noted
		New hires and other new system access requirements are approved as part of the onboarding process or by authorized system owners prior to access being granted.	Inspected the access approval for a sample of new hires to determine that new hires and other new system access requirements were approved as part of the onboarding process or by authorized system owners prior to access being granted.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	segregation of duties, to meet the entity's objectives.	A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner.	No exceptions noted.
		Quarterly reviews of Exa's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required.	Inspected the user access review for a sample of quarters to determine that quarterly reviews of Exa's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required.	No exceptions noted
		Exa requires appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	Inspected the access control policy to determine that Exa required appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by 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.	A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner.	No exceptions noted.
		Quarterly reviews of Exa's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required.	Inspected the user access review for a sample of quarters to determine that quarterly reviews of Exa's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed.	Inspected the secure disposal policies and procedures to determine that the disposal of sensitive information assets followed a defined process to ensure sensitive data was effectively erased before the safeguards over the information assets were removed.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Exa implements network access restrictions that ensure only approved communication channels and protocols can be used.	Inspected the network access restrictions to determine that Exa implemented network access restrictions that ensured only approved communication channels and protocols could be used.	No exceptions noted
		Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted
		Connections and data flows to the Software as a Service System and the supporting infrastructure are encrypted in transit.	Inspected the encryption in transit configurations to determine that connections and data flows to the Software as a Service System and the supporting infrastructure were encrypted in transit.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Multi-factor authentication is required for access to sensitive systems.	Inspected the monitoring of multi-factor authentication to determine that multi-factor authentication was required for access to sensitive systems.	No exceptions noted
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
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,	Exa stores sensitive data, including customer data, in databases that are encrypted at rest.	Inspected the database encryption to determine that Exa stored sensitive data, including customer data, in databases that were encrypted at rest.	No exceptions noted
		Connections and data flows to the Software as a Service System and the supporting infrastructure are encrypted in transit.	Inspected the encryption in transit configurations to determine that connections and data flows to the Software as a Service System and the supporting infrastructure were encrypted in transit.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	movement, or removal to meet the entity's objectives.	Antivirus software is installed on workstations to protect against malware.	Inspected the monitoring of antivirus software installed on workstations to determine that antivirus software was installed on workstations to protect against malware.	No exceptions noted
		Exa's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	Inspected the monitoring of hard-disk encryption for devices to determine that Exa's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	No exceptions noted
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	unauthorized or malicious software to meet the entity's objectives.	Antivirus software is installed on workstations to protect against malware.	Inspected the monitoring of antivirus software installed on workstations to determine that antivirus software was installed on workstations to protect against malware.	No exceptions noted
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

Common Criteria 7: System Operations

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa uses a version control system to manage source code, documentation, release labelling, and other change management tasks.	Inspected the version control software to determine that Exa used a version control system to manage source code, documentation, release labelling, and other change management tasks.	No exceptions noted
		Changes are automatically tested and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production.	Inspected the configuration of the CI/CD pipeline to determine that changes were automatically tested and approval flows verified in the configured continuous integration/continuous deployment (CI/CD) software before they could be promoted to production.	No exceptions noted
		Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted
		Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Independent penetration tests are conducted annually.	Inspected the penetration test report to determine that independent penetration tests were conducted annually.	No exceptions noted
		Exa defines the approach to identifying, assessing and resolving security vulnerabilities.	Inspected the vulnerability management policy to determine that Exa defined the approach to identifying, assessing and resolving security vulnerabilities.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
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.	Information logs related to the information processing activities are centrally stored for retrospective analysis where required.	Inspected the configuration of log capture to determine that information logs related to the information processing activities were centrally stored for retrospective analysis where required.	No exceptions noted
		Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted
		Vanta is used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	Inspected the Vanta monitoring to determine that Vanta was used to continuously monitor the security and compliance of Exa's information assets including its people, systems, and control framework.	No exceptions noted

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted
		Independent penetration tests are conducted annually.	Inspected the penetration test report to determine that independent penetration tests were conducted annually.	No exceptions noted
		Exa defines the approach to identifying, assessing and resolving security vulnerabilities.	Inspected the vulnerability management policy to determine that Exa defined the approach to identifying, assessing and resolving security vulnerabilities.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
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,	Exa follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident handling for a sample of incidents to determine that Exa followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	No exceptions noted

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	takes actions to prevent or address such failures.	Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain,	The incident response plans are reviewed at least annually to confirm they provide an effective response to potential incidents.	Inspected the annual review of the incident response plans to determine that the incident response plans were reviewed at least annually to confirm they provided an effective response to potential incidents.	No exceptions noted

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	remediate, and communicate security incidents, as appropriate.	Exa follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident handling for a sample of incidents to determine that Exa followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	No exceptions noted
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Daily backups are performed and monitored to support recoverability of the production data.	Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data.	No exceptions noted
		The incident response plans are reviewed at least annually to confirm they provide an effective response to potential incidents.	Inspected the annual review of the incident response plans to determine that the incident response plans were reviewed at least annually to confirm they provided an effective response to potential incidents.	No exceptions noted

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident handling for a sample of incidents to determine that Exa followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	No exceptions noted
		Exa conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.	Inspected the business continuity and disaster recovery tests to determine that Exa conducted annual business continuity and disaster recovery tests to ensure the response plans were effective.	No exceptions noted
		Exa establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine Exa established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities.	No exceptions noted
		The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems.	Inspected the disaster recovery plans to determine that the established disaster recovery plans outlined roles, responsibilities, and detailed procedures for the recovery of critical systems.	No exceptions noted

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa documents the scenarios and relevant impacts that may threaten Exa's continuity, as well as the roles, responsibilities, and plans to manage those events effectively.	Inspected the business continuity plans to determine that Exa documented the scenarios and relevant impacts that may threaten Exa's continuity, as well as the roles, responsibilities, and plans to manage those events effectively.	No exceptions noted
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

Common Criteria 8: Change Management

CC8.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Exa uses a version control system to manage source code, documentation, release labelling, and other change management tasks.	Inspected the version control software to determine that Exa used a version control system to manage source code, documentation, release labelling, and other change management tasks.	No exceptions noted
		When Exa's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected the systematic enforcement of peer reviews to determine that when Exa's application code changes, code reviews and tests were performed by someone other than the person who made the code change.	No exceptions noted
		Only authorized Exa personnel can deploy changes into production.	Inspected the access restrictions and roles to determine that only authorized Exa personnel could deploy changes into production.	No exceptions noted
		Changes are automatically tested and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production.	Inspected the configuration of the CI/CD pipeline to determine that changes were automatically tested and approval flows verified in the configured continuous integration/continuous deployment (CI/CD) software before they could be promoted to production.	No exceptions noted

CC8.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Separate environments are used for testing and production for Exa's Software as a Service System.	Inspected the separation of environments to determine that separate environments were used for testing and production for Exa's Software as a Service System.	No exceptions noted
		Exa has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the policies and procedures to determine that Exa had developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

Common Criteria 9: Risk Mitigation

CC9.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Daily backups are performed and monitored to support recoverability of the production data.	Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data.	No exceptions noted
		Exa implements infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	Inspected the redundancy configurations to determine that Exa implemented infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	No exceptions noted
		Exa follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident handling for a sample of incidents to determine that Exa followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.	No exceptions noted
		Exa conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.	Inspected the business continuity and disaster recovery tests to determine that Exa conducted annual business continuity and disaster recovery tests to ensure the response plans were effective.	No exceptions noted

CC9.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa maintains cybersecurity insurance to mitigate the impact of potential data breaches and disruptions.	Inspected the cybersecurity insurance to determine that Exa maintained cybersecurity insurance to mitigate the impact of potential data breaches and disruptions.	No exceptions noted
		Exa conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	Inspected the risk assessments to determine that Exa conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.	No exceptions noted
		Exa's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	Inspected the risk remediation plan to determine that Exa's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.	No exceptions noted
		Exa has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	Inspected the risk assessment policy to determine that Exa had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.	No exceptions noted

CC9.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems.	Inspected the disaster recovery plans to determine that the established disaster recovery plans outlined roles, responsibilities, and detailed procedures for the recovery of critical systems.	No exceptions noted
		Exa documents the scenarios and relevant impacts that may threaten Exa's continuity, as well as the roles, responsibilities, and plans to manage those events effectively.	Inspected the business continuity plans to determine that Exa documented the scenarios and relevant impacts that may threaten Exa's continuity, as well as the roles, responsibilities, and plans to manage those events effectively.	No exceptions noted
		Exa defines the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	Inspected the incident response plans to determine that Exa defined the roles, responsibilities and communication requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.	No exceptions noted
		Exa establishes the requirements for backups and recoverability.	Inspected the backup policy to determine that Exa established the requirements for backups and recoverability.	No exceptions noted

CC9.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.	Inspected the vendor register to determine that the vendor register included material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.	No exceptions noted
		Exa performs security and compliance assessments of critical and high-risk vendors.	Inspected the security and compliance review for a sample of critical and high-risk vendors to determine that Exa performed security and compliance assessments of high-risk vendors.	No exceptions noted
		Exa sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	Inspected the vendor management policy to determine that Exa set out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.	No exceptions noted

Additional Criteria for Availability

A1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Auto-scaling configuration is used to automatically provision additional capacity when predefined thresholds are met.	Inspected the auto-scaling configuration to determine that auto-scaling configuration was used to automatically provision additional capacity when predefined thresholds were met.	No exceptions noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and	Daily backups are performed and monitored to support recoverability of the production data.	Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data.	No exceptions noted
		Exa implements infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	Inspected the redundancy configurations to determine that Exa implemented infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	No exceptions noted

A1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	recovery infrastructure to meet its objectives.	Exa conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.	Inspected the business continuity and disaster recovery tests to determine that Exa conducted annual business continuity and disaster recovery tests to ensure the response plans were effective.	No exceptions noted
		The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems.	Inspected the disaster recovery plans to determine that the established disaster recovery plans outlined roles, responsibilities, and detailed procedures for the recovery of critical systems.	No exceptions noted
		Exa establishes the requirements for backups and recoverability.	Inspected the backup policy to determine that Exa established the requirements for backups and recoverability.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Daily backups are performed and monitored to support recoverability of the production data.	Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data.	No exceptions noted
		Exa conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.	Inspected the business continuity and disaster recovery tests to determine that Exa conducted annual business continuity and disaster recovery tests to ensure the response plans were effective.	No exceptions noted

Additional Criteria for Confidentiality

C1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Employment contracts are formed with Exa employees including a non-disclosure agreement (NDA) for confidential information.	Inspected the employment contracts for a sample of new hires to determine that employment contracts were formed with Exa employees including a non-disclosure agreement (NDA) for confidential information.	No exceptions noted
		Exa requires appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	Inspected the access control policy to determine that Exa required appropriate access approvals based on role-based access control and the principle of least privilege, periodic user access reviews, and timely revocation of access upon termination, to ensure access is restricted to authorized personnel.	No exceptions noted
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted
		Exa establishes the data types and retention periods of data collected and processed.	Inspected the data retention policies to determine that Exa established the data types and retention periods of data collected and processed.	No exceptions noted

C1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Exa establishes the method of data classification to ensure appropriate protections are applied based on its sensitivity.	Inspected the data classification policies to determine that Exa established the method of data classification to ensure appropriate protections were applied based on its sensitivity.	No exceptions noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner.	No exceptions noted.
		Exa establishes the boundaries and requirements for how employees use Exa's systems and information assets to protect against data leakage, malware, and security breaches.	Inspected the acceptable use policy to determine that Exa established the boundaries and requirements for how employees used Exa's systems and information assets to protect against data leakage, malware and security breaches.	No exceptions noted
		The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed.	Inspected the secure disposal policies and procedures to determine that the disposal of sensitive information assets followed a defined process to ensure sensitive data was effectively erased before the safeguards over the information assets were removed.	No exceptions noted