



SNYK INC.

SOC 2 REPORT

FOR

SNYK PLATFORM

**A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY**

JUNE 1, 2024, TO MAY 31, 2025

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of Snyk Inc., user entities of Snyk Inc.'s services, and other parties who have sufficient knowledge and understanding of Snyk Inc.'s services covered by this report (each referred to herein as a "specified user").

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2 MANAGEMENT'S ASSERTION	5
SECTION 3 DESCRIPTION OF THE SYSTEM	7
SECTION 4 TESTING MATRICES	22
SECTION 5 OTHER INFORMATION PROVIDED BY SNYK.....	60

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Snyk Inc.:

Scope

We have examined Snyk Inc.'s ("Snyk" or the "service organization") accompanying description of its Snyk Platform system, in Section 3, throughout the period June 1, 2024, to May 31, 2025, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2024, to May 31, 2025, to provide reasonable assurance that Snyk'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Snyk uses various subservice organizations for cloud hosting and database management services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Snyk, to achieve Snyk's service commitments and system requirements based on the applicable trust services criteria. The description presents Snyk's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Snyk's controls. The description does not disclose the actual controls at the subservice organizations. 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 information included in Section 5, "Other Information Provided by Snyk" is presented by Snyk management to provide additional information and is not a part of the description. Information about Snyk's API and Web systems has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Snyk's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and 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 Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

- the description presents Snyk's Platform system that was designed and implemented throughout the period June 1, 2024, to May 31, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period June 1, 2024, to May 31, 2025, to provide reasonable assurance that Snyk's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Snyk's controls throughout that period; and

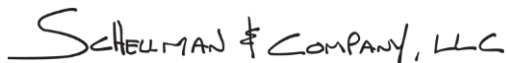
- the controls stated in the description operated effectively throughout the period June 1, 2024, to May 31, 2025, to provide reasonable assurance that Snyk's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Snyk's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Snyk; user entities of Snyk's Platform system during some or all of the period of June 1, 2024, to May 31, 2025, business partners of Snyk subject to risks arising from interactions with the Snyk Platform 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 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; and
- 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.

 SCHEELMAN & COMPANY, LLC

Tampa, Florida
July 8, 2025

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Snyk's Platform system, in Section 3, throughout the period June 1, 2024, to May 31, 2025, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Snyk Platform system that may be useful when assessing the risks arising from interactions with Snyk's system, particularly information about system controls that Snyk 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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

- the description presents Snyk's Platform system that was designed and implemented throughout the period June 1, 2024, to May 31, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period June 1, 2024, to May 31, 2025, to provide reasonable assurance that Snyk's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Snyk's controls throughout that period; and
- the controls stated in the description operated effectively throughout the period June 1, 2024, to May 31, 2025, to provide reasonable assurance that Snyk's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Snyk's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Snyk was founded in 2015 and is headquartered in Boston, Massachusetts. Snyk has over 1,000 employees with additional offices in Bucharest, Cluj, Lisbon, London, Ottawa, Singapore, Sydney, Tel Aviv, Tokyo, and Zurich. The Snyk Platform helps companies stay secure by finding, fixing, preventing, and continuously monitoring applications for known vulnerabilities. The platform also provides integrations with source code managers, bringing security workflows to developers' current tools rather than requiring them to learn new tools.

Description of Services Provided

Snyk offers the following tools and services:

- Interfaces
 - Snyk web application – Snyk's web application is a software-as-a-service (SaaS) offering that allows for easy integration with source code managers (SCMs) like GitHub and provides a dashboard where users can view their applications and the existing vulnerabilities, as well as invoke a fix pull request to remediate vulnerabilities. Reports showing vulnerability counts, exposure windows, and trends provide clarity into a customer's security posture. Bill of materials (BOMs) reports allow customers to gain visibility into the various open-source packages throughout their portfolio.
 - Snyk Broker – Snyk Broker allows customers to work in a hybrid mode, allowing them to connect their on-premises SCM to Snyk. The broker, which is set up by the customer in their environment, acts as a proxy to allow for communication between the on-premises SCM and Snyk. In addition, Snyk Broker acts as a data leak prevention (DLP) solution, allowing only whitelisted data flows to enter or exit the network, thus ensuring that the customer's code and SCM credentials never leave the customer's network.
 - Snyk Command Line Interface (CLI) – Snyk CLI allows customers to scan applications in the context of a continuous integration (CI) pipeline or on a developer's machine.
 - Snyk Application Programming Interface (API) – Snyk API allows for ad-hoc testing of packages or entire manifest files via a programmatic interface. The API also allows customers to extract reporting data directly from the Snyk Platform, making it easy for customers to pull this data into their own dashboarding tools and reports.
- Core Product Offerings
 - Snyk Open Source – Snyk Open Source allows developers to automatically find, prioritize, and fix vulnerabilities in the open-source dependencies used to build customer applications.
 - Snyk Container – Snyk Container allows developers to easily find and fix vulnerabilities in container images and Kubernetes applications.
 - Snyk Infrastructure as Code (IaC) – Snyk IaC helps developers ship secure applications and infrastructure faster by embedding IaC security for Terraform, CloudFormation, Kubernetes, Helm charts, and Azure Resource Manager (ARM) templates within an integrated development environment (IDE), CLI, software configuration management, and CI / continuous deployment (CD) workflows.
 - Snyk Code – Snyk Code provides static application security testing for developers, assisting them in finding and fixing code vulnerabilities.
 - Snyk AppRisk – Snyk AppRisk enables Application Security teams to reduce application risk with complete application discovery, tailored security controls, and risk-based prioritization.

Snyk offers both multi-tenant and single tenant offerings for its customers. The single tenant environment separates data and compute resources for its customers.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments

Snyk has put into place a set of policies and procedures to help ensure that security, availability, and confidentiality commitments are met. Snyk's commitments to user entities are described in the customer services agreements (SAs). Snyk communicates its service level agreement (SLA) commitments through the SA with customers during the contractual agreement process. The SLA and SA terms are specific to the services purchased by the customer. Snyk makes the following principal service commitments to its customers:

- To the extent permissible under applicable local law, Snyk shall use a reputable third-party service provider to perform employment history and criminal background checks on employees.
- Snyk shall maintain a cyber-liability insurance policy.
- Services will perform substantially in accordance with the agreement and support will be performed with reasonable skill and care.
- In the event of a breach of security resulting in an unauthorized or unlawful destruction, loss, alteration, disclosure of, or access to, customer data, upon becoming aware of the security incident, Snyk will take reasonable action to mitigate the security incident and notify affected parties without undue delay, as necessary.
- Snyk will hold the customer's confidential information in confidence unless required by law to be disclosed and will not use the information for any purpose other than as set out in the agreement.
- Snyk shall endeavor to ensure that the services are available to customers 99.9% of the time.
- Snyk shall ensure that appropriate levels of backups are in place to support customer data confidentiality, integrity, and availability requirements.
- Snyk's security program includes administrative and technical safeguards reasonably designed to protect the confidentiality, integrity, and availability of customer data.
- Snyk uses industry-standard encryption techniques to encrypt customer data at rest and in transit.
- Snyk provides status updates, service interruptions, information regarding upgrades, new release availability, minimum release version requirements to the publicly available status page.
- Snyk maintains a data retention standard and enforces the standard such that customer data backups are retained in accordance with policy, after which they are deleted from the backup location.

System Requirements

Snyk regularly reviews security metrics to help ensure the principal service commitments are met. Snyk establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Snyk's system policies and procedures and system design documentation. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the services.

In accordance with the assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to each system user, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

The infrastructure and software supporting the Snyk system is maintained at third-party data center facilities operated by AWS and Google across the US-East region. Data is replicated in real-time across multiple availability zones within the aforementioned region. The Snyk Platform utilizes Amazon Elastic Container Service (ECS) and Google Kubernetes Engine (GKE) for managed container services, and MongoDB and Snowflake for database-as-a-service (DBaaS). Snyk operates under a shared security responsibility model where AWS, Google, MongoDB, and Snowflake are responsible for the security of the underlying cloud and database infrastructure (e.g., physical infrastructure, geographical regions, availability zones, edge locations), and Snyk is responsible for securing the platform deployed with AWS and Google (e.g., customer data, applications, access management, operating system layer, etc.) and data stored within MongoDB and Snowflake.

The in-scope infrastructure consists of multiple applications, operating system platforms, and databases, as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Operating System Platform	Physical Location
Snyk Platform	Developer security platform.	AWS Google	AWS Google
Identity Access Management (IAM) and Single Sign-On (SSO) Provider	Vendor provided secure identity management and single sign-on.	Vendor Managed	Vendor Managed
Just-in-Time Access Tool	Managed secure shell (SSH) jump server solution.		
AWS IAM	Enables secure control of access to AWS services and resources for users.	AWS	AWS
Amazon ECS	Managed container orchestration service used to deploy, manage, and scale containerized applications.		
Amazon Relational Database Service (RDS)	Database solution for storage of operational data.	MySQL	
Amazon Simple Storage Service (S3)	Highly resilient and available file based datastore for backup, redundancy, and customer data.	AWS	

Primary Infrastructure			
Production System	Business Function Description	Operating System Platform	Physical Location
Google Admin Console	Enables secure control of access to Google services and resources for users.	Google	Google
GKE	Managed container orchestration service used to deploy, manage, and scale containerized applications.		
Google Cloud SQL	Scalable, managed database available on GCP.		
MongoDB Atlas	Managed database services.	Vendor Managed	Vendor Managed
Snowflake	Managed database and data warehouse services.		

People

Snyk develops, manages, and secures the Snyk Platform via separate departments. The responsibilities of these departments are defined below:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
- Engineering – responsible for the infrastructure supporting the development, testing, and deployment environments, and maintenance of new code.
- Information Security (InfoSec) – Responsible for the development, implementation, and maintenance of business security standards and principles to ensure a secure business environment and continual improvement.
- Information Technology (IT) – responsible for the internal tools, corporate IT and support, information security, and application security needed for Snyk to enable employees to work.
- Governance, Risk, and Compliance (GRC) – responsible for ensuring adequate Governance, Risk, and Compliance practices are implemented at Snyk, with the aim of continued improvement and maturity.
- Product – Responsible for overseeing the product life cycle, including adding new product functionality.
- People – Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.
- Finance, Legal, and Procurement – Responsible for Snyk's legal, financial, and control activities, including financial planning and administrative tasks, as well as hiring. The team is responsible for sourcing and acquiring the goods and services that Snyk needs to operate efficiently, as well as ensuring that new vendors go through the appropriate legal and security assessments prior to completion of the contract. The team maintains relevant contractual terms and ensures that security addendums are implemented and retained.

Procedures

Access, Authentication, and Authorization

Access to the production systems is governed by IT policies and procedures. In order to access the production systems, users authenticate via a unique user account, password, and multi-factor authentication (MFA) or SSH keypair via Teleport jump server. Access to the public-facing application is encrypted via transport layer security (TLS). TLS is provisioned as part of the default installation to help ensure secure transmission over the Internet for the platform. Predefined security groups are utilized to assign role-based access privileges and restrict access to data within the in-scope systems.

Access to administer the production systems is restricted to authorized personnel. Additionally, user access reviews, including privileged users, are performed by management on a quarterly basis to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.

Access Requests and Access Revocation

When a new employee is hired, the hiring manager and human resources (HR) personnel complete an onboarding checklist within the HR system to request user access for the new employee. System access is provisioned once the checklist is reviewed and approved by IT personnel. Documented position descriptions are utilized to help guide newly hired personnel in understanding their roles and responsibilities for their position. Existing employees who require system access changes are required to submit requests in writing to the ticketing system, and upon approval, access is granted within the respective system.

Upon notification of employee termination, a member of the IT team revokes the terminated employee's system access, as well as privileged system access to the in-scope systems. Employee termination activities are documented within an offboarding ticket.

Network Security and Endpoint Protection

The production network is logically segmented to help ensure that confidential data is isolated from other unrelated networks. A web application firewall (WAF) is utilized to monitor and analyze web application events for possible or actual security breaches, and filter, monitor, and block inbound and outbound traffic from the Internet. Security groups are in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule. Mobile device management (MDM) software is configured to encrypt the hard drives of Snyk-owned workstations. Endpoint detection and response (EDR) software is configured to install and manage the enterprise antivirus software on Snyk-owned workstations and enforces behavior-based prevention policies to prevent the introduction of unauthorized or malicious software. The EDR software is configured to be automatically updated on a continuous basis. Additionally, the ability to install applications or software is restricted to authorized engineering personnel.

Change Management

Documented change management policies and procedures are in place to guide personnel in the systems development and change management processes, including submitting change requests, change request prioritization, and approving change requests. A combination of the version control system and a ticketing system are utilized to maintain, manage, and monitor enhancement, development, and maintenance activities and to document change requests from initiation through implementation. The production change request process records request authorization, code review, testing, migration approvals, and implementation details. Emergency changes follow the standard change management process. Production customer data is not utilized for development or testing in non-production environments. Additionally, the production environment is logically segmented from development and test environments.

A version control system is utilized to control access to source code and is configured to require peer review and approval by personnel other than the author of the change prior to changes being merged into the production code branch. The ability to modify source code libraries within the version control software is restricted to user accounts accessible by authorized engineering personnel. Administrative access privileges to the version control software and access to deploy changes into the production environment are restricted to user accounts accessible by authorized personnel.

An automated deployment tool is in place and configured to alert operations personnel via the internal team collaboration tool when deployments to production occur. Access to modify the automated deployment tool is restricted to authorized personnel.

Data Backup and Disaster Recovery

Snyk maintains documented policies and procedures to guide personnel in back-up processes, recovering data, and handling of stored data. Production data is replicated across separate availability zones. Automated backup systems are in place to perform backups of customer data on at least a daily basis, are configured to retain backups for up to 90 days, and are stored in an encrypted format.

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and are reviewed, updated, and approved on an annual basis. Disaster recovery plans are tested on an annual basis to help ensure Snyk can recover in the event of a disaster. Engineering personnel perform backup data restores on an annual basis to help ensure that system components can be recovered from system backups.

System Monitoring

Snyk has various monitoring tools in place to detect anomalies in the system. A host-based intrusion detection system (HIDS) is utilized to analyze and report network events and to block suspected or actual network security breaches. Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.

On an annual basis, penetration testing is performed by a third-party vendor. A third-party utility is configured to perform vulnerability scans on a daily basis. The results of the penetration test and vulnerability scans are reviewed by management to devise remediation plans to address emerging security risks. A bug bounty program is also in place to identify threats and assess their potential impact to the system. Reported vulnerabilities are reviewed by Information Security personnel and monitored through resolution as needed. Additionally, Information Security personnel monitor the security impact of emerging technologies and senior management considers the impact of applicable laws and regulations.

Incident Response

Documented escalation procedures for reporting incidents are provided to employees to guide users in identifying and reporting system failures, incidents, concerns, and other complaints. Incident review meetings are held to help ensure the alignment of information security and business objectives, discuss the effect of identified security vulnerabilities on the ability to meet business objectives, respond to security incidents, and identify corrective measures. For any confirmed security incidents, a security incident report is created to document the incident, response, and resolution. Reported or detected security incidents are tracked within a ticketing system until resolved. Closed security incidents are reviewed and approved by management to help ensure that the incident response procedures were followed, and that the incident was resolved. The incident response plan is also tested at least annually to assess the effectiveness of the incident response program.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by Snyk. Through the API, the customer or end-user defines and controls the data they load into and store in the Snyk Platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Data is managed and processed according to Snyk's data protection policies and procedures. Documents are marked according to their sensitivity and usage, and access to data and systems is only granted based on a business need-to-know. Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts.

Customer data is not utilized for testing in non-production environments. Confidential data is encrypted at rest. The transmission of confidential data is secured via an Internet connection encrypted with TLS protocol. Documented data classification and retention policies are in place to help ensure that confidential data is properly maintained, restricted to authorized personnel, and prohibited from being used or stored outside of company-approved methods. Snyk has established a data retention standard to retain backup data for current customers. Snyk enforces the standard such that customer data backups are retained for up to 90 days after which they are deleted from the backup location.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Vulnerability data	Snyk stores information on the vulnerabilities identified in customers' applications and related remediation context.	Confidential
Vulnerability source	Snyk stores information on where vulnerabilities were identified (e.g., source code repository / registry, file name and location, dependency tree, vulnerability path).	
Integration-related data	Snyk stores information required to set up an integration with Snyk (e.g., tokens, configurations).	
User data	Snyk stores basic user information (e.g., username, ID, e-mail address).	
User list	For the purposes of an accurate contributor counting, Snyk accesses commits from the last 90 days for monitored repositories and stores a hashed version of user e-mails.	
User behavior analytics	Snyk stores various types of information pertaining to usage patterns (e.g., website visits, executed CLI commands).	

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting and database management services provided by AWS, Google, MongoDB, and Snowflake were not included within the scope of this examination.

The following table presents the applicable trust services criteria that are intended to be met by controls at AWS, Google, MongoDB, and Snowflake, alone or in combination with controls at Snyk, and the types of controls expected to be implemented at AWS, Google, MongoDB, and Snowflake to achieve Snyk's principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.	CC6.1 – CC6.3 CC6.5 – CC6.6 C1.1

Ref.	Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
CSOC.02	MongoDB and Snowflake are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.	CC6.1 – CC6.3 CC6.6, C1.1
CSOC.03	Google and Snowflake are responsible for ensuring data within GCP and Snowflake are stored in an encrypted at rest format.	CC6.1, C1.1
CSOC.04	AWS, Google, MongoDB, and Snowflake are responsible for ensuring access to server-side encryption keys is restricted to authorized personnel.	
CSOC.05	AWS and Google are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
CSOC.06	AWS and Google are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the Snyk systems reside.	CC6.7
CSOC.07	AWS and Google are responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.	CC7.2
CSOC.08	MongoDB and Snowflake are responsible for monitoring the logical access control systems for the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.	
CSOC.09	AWS, Google, MongoDB, and Snowflake are responsible for monitoring the capacity demand and ensuring capacity resources are available and functioning to meet Snyk's availability commitments and requirements.	A1.1
CSOC.10	AWS and Google are responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing a monitoring application to monitor for environmental events.	A1.2
CSOC.11	Snowflake is responsible for performing scheduled backups and replication of Snowflake databases to multiple diverse locations at predefined times.	

CONTROL ENVIRONMENT

The control environment at Snyk is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence, its organizational structure, the assignment of authority and responsibility, and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

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

through policy statements and codes of conduct. Specific control activities that Snyk has implemented in this area are described below:

- Management formally documents and reviews the organizational policy statements that communicate entity values and behavioral standards to personnel.
- Employees are required to sign an acknowledgment form upon hire and on an annual basis, thereafter, indicating that they have been given access to the employee code of conduct and information security policies, which includes standards of employee conduct, and they understand their responsibility for adhering to the associated policies and procedures.
- Employees are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background screening is performed for employment candidates as a component of the hiring process.
- An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.

Board of Directors and Executive Management Oversight

Snyk's control awareness is influenced significantly by its executive management team and board of directors. Attributes include the experience and stature of its members, the extent of its involvement and scrutiny of operational activities, the degree to which difficult questions are raised and pursued with management, and their interaction with external auditors. Specific control activities that Snyk has implemented in this area are described below:

- The board of directors establishes and maintains oversight of management's system of internal control.
- The board of directors has members who are independent from management and are objective in evaluations and decision making.
- Board of directors and committee meetings are held on a quarterly basis to review internal control performance.
- Internal control performance metrics are provided to information security management system (ISMS) management on an annual basis. These metrics are documented in summary presentations for ISMS management review.

Organizational Structure and Assignment of Authority and Responsibility

Snyk's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Snyk has developed an organizational structure suited to its needs. Snyk's organizational structure depends, in part, on its size and the nature of its activities. This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. Policies and communications are in place to help ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that Snyk has implemented in this area are described below:

- The organizational structure, reporting lines, and authorities are defined in organizational charts, updated on an as needed basis, and communicated to employees via the company intranet.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- A security team that is composed of operations personnel and executive staff has been established to guide the company in managing security risks.
- Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the Chief Information Security Officer (CISO).

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Snyk's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that Snyk has implemented in this area are described below:

- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Employees are required to complete security awareness training, upon hire and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Management personnel monitor compliance with security awareness training requirements on an ongoing basis.
- Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
- Employee performance reviews are conducted at least annually to evaluate employees against expected levels of performance.

Accountability

Management establishes accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against, as well as incentives and other rewards. Specific control activities that Snyk has implemented in this area are described below:

- Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.
- Employee performance reviews are conducted at least annually to evaluate employees against expected levels of performance.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.
- A security team that is composed of operations personnel and executive staff has been established to guide the company in managing security risks.
- Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.

RISK ASSESSMENT

Management is responsible for identifying relevant risks which threaten the organization's ability to provide reliable service for user entities. The risk assessment process, facilitated in collaboration with Snyk management by the GRC team, includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them.

Objective Setting

A risk assessment is performed at least annually that identifies and evaluates changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of objectives. Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to help ensure they align with the company's mission and are utilized as part of the risk assessment process.

Risk Identification and Analysis

Snyk assesses risks from external interactions that could impact service reliability for users. System security threats are identified, evaluated, and formally assessed. Management and operational teams annually identify and review system risks, formally documenting them in the risk register. The process is documented, maintained, and remediation activities are management-approved.

Risk analysis is crucial for Snyk's success. It identifies key business processes with potential exposures and significant changes. After assessing risk significance and likelihood, management determines how to manage it, involving judgment based on risk assumptions and cost-benefit analysis for reduction. Actions are taken to reduce risk significance or likelihood, and control activities are identified to mitigate it. Additionally, management periodically reviews assessed risk levels and documents the assessment in the risk program.

Risk Factors

Management considers risks that can arise from both external and internal factors including, but not limited to, the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, including fraud incentives, pressures, opportunities, attitudes, and rationalizations for employees
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

The risk assessment evaluates the potential for fraud, both in financial and non-financial reporting, and its impact on achieving objectives. Management understands that fraud can be driven by employee pressures or incentives, and facilitated by absent or ineffective controls. Therefore, potential fraud risks are identified during the assessment, and management determines the appropriate response.

Risk Mitigation

Risk mitigation strategies involve internal controls (prevention / elimination) and insurance (transference). Management is responsible for identifying and mitigating significant risks in their areas, guided by documented policies and procedures. This process also addresses potential business disruption risks.

Vendors and business partners are included in the risk assessment and mitigation process, with documented policies guiding risk identification. Management annually reviews vendor audit reports for compliance. Confidential information shared with third parties requires signed Master Service Agreements (MSAs) with specific confidentiality and protection terms.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

Selection and Development of Control Activities

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Snyk's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Snyk Platform system.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of Snyk's internal control system. They include the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the organization's operations. At Snyk, information is identified, captured, processed, and reported by various information systems, as well through conversations with clients, vendors, regulators, and employees. Management obtains or generates and uses relevant information from both internal and external sources to support the functioning of internal controls.

Internal Communications

Snyk has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for employees, and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate to their direct supervisor or senior management. A code of conduct, information security policy, and acceptable use policy for reporting operational failures, incidents, system problems, concerns, and user complaints are documented by Snyk management, reviewed, approved annually, published, and made available on the company intranet. Additionally, management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives. Senior executives who lead these meetings use information gathered from formal, automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to company-wide security policies and procedures are communicated to the appropriate personnel via Slack notifications and shared with the appropriate audience using Snyk's intranet. Snyk's content management application serves as an internal sharing platform for relevant information with Snyk's employees. An anonymous hotline for the communication of complaints is accessible by internal users to report incidents, concerns, and complaints.

External Communications

Snyk has also implemented various methods of communication to help provide assurance that user entities understand their roles and responsibilities in communication of significant events. Snyk utilizes the public-facing website to communicate relevant information regarding the design and operation of the system and Snyk's commitments to external customers. External release notes are published in the public repository for Snyk.io. Additionally, service interruptions, maintenance, and updates are communicated to customers through the Snyk portal status page. The website also features a portal where customers can communicate with Snyk for support of the system or to report any incidents or concerns related to the operation or security of the system.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two.

Management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control activities and procedures to help ensure they are operating as intended and are modified for changes in conditions, as necessary. Management places emphasis on maintaining sound internal controls, as well as ensuring the integrity and ethical values of Snyk personnel. Senior management develops action plans to address any internal control or quality assurance (QA) areas that need attention. Management reviews these action plans on a periodic basis.

Ongoing Monitoring

Snyk uses a suite of monitoring tools to monitor its services. Management performs ongoing monitoring and deficiencies are identified by continuous monitoring and periodic reviews of controls through alerts, reports, checklists, as well as management and peer reviews. Alerts are sent to relevant stakeholders based on predefined rules. A third-party utility is utilized to perform vulnerability scans on a daily basis, and penetration testing is performed annually. Management uses automated reports created through various applications and processes to monitor the efficiency of certain processes and the effectiveness of certain key controls. Metrics produced from these systems are used to identify the strengths and achievements, as well as the weaknesses, inefficiencies, or potential performance issues, with respect to a process. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time. The management team monitors the progress with respect to Snyk's service processes regularly. An analysis of the root cause of issues is performed through various tools and meetings, and corrective measures are communicated to relevant groups through e-mails, meetings, and a project portal tool to prevent future occurrences. Further monitoring, review, and training processes are improved to prevent recurrence.

Separate Evaluations

Internal audits are performed by management at least annually to gain assurance that controls are in place and operating effectively. Additionally, external assessments are performed on specific areas of control in accordance with management objectives and business strategy. Corrective actions are taken by management based on relevant findings and tracked to resolution. The findings of these efforts are utilized to help ensure follow-up actions are taken and subsequent evaluations are modified, as necessary.

Subservice Organization Monitoring

Snyk management reviews third-party vendor contract agreements and annual service auditor's reports, as applicable, on an annual basis to help ensure that third-party providers comply with security, availability, and confidentiality policies. In the event that an issue is identified within the audit reports, Snyk security management would schedule a meeting with their third-party representative to review and discuss the issue.

Evaluating and Communicating Deficiencies

Deficiencies in management's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person.

Management tracks related deficiencies on an ongoing basis. This process enables management to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected.

System Incident Disclosures

No system incidents occurred that were the result of controls that were not suitably designed or operating effectively or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements during the period.

COMPLEMENTARY CONTROLS AT USER ENTITIES

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

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Snyk Platform system provided by Snyk. The scope of the testing was restricted to the Snyk Platform system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period June 1, 2024, through May 31, 2025.

Tests of Operating Effectiveness

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

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

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

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

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

Reliability of Information Provided by the Service Organization

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

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria, are presented in the “Subservice Organizations” section within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Management formally documents and reviews the organizational policy statements that communicate entity values and behavioral standards to personnel.	Inspected the code of conduct to determine that management formally documented and reviewed the organizational policy statements that communicated entity values and behavioral standards to personnel.	No exceptions noted.
CC1.1.2	Employees are required to sign an acknowledgment form upon hire and on an annual basis, thereafter, indicating that they have been given access to the employee code of conduct and information security policies, which includes standards of employee conduct, and they understand their responsibility for adhering to the associated policies and procedures.	Inspected the signed acknowledgment form for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgment form upon hire indicating that they had been given access to the employee code of conduct and information security policies, which included standards of employee conduct, and that they understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the signed acknowledgment form for a sample of employees to determine that each employee sampled signed an acknowledgment form during the period indicating that they had been given access to the employee code of conduct and information security policies, which included standards of employee conduct, and they understood their responsibility for adhering to the associated policies and procedures.	No exceptions noted.
CC1.1.3	Employees are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreement for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC1.1.4	Background screening is performed for employment candidates as a component of the hiring process.	Inspected the background screening documentation for a sample of employees hired during the period to determine that background screening was performed as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.1.5	An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the disciplinary action policy and procedure to determine that an employee sanction policy was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	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.			
CC1.2.1	The board of directors establishes and maintains oversight of management's system of internal control.	Inspected the board of directors' charter to determine that the board of directors established and maintained oversight of management's system of internal control.	No exceptions noted.
CC1.2.2	The board of directors has members who are independent from management and are objective in evaluations and decision making.	Inspected the listing of board of directors members and the employee listing to determine that the board of directors had members who were independent from management and objective in evaluations and decision making.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.3	Board of directors and committee meetings are held on a quarterly basis to review internal control performance.	Inspected the board of directors meeting calendar invitation and the meeting agenda for a sample of quarters during the period to determine that board of directors and committee meetings were held to review internal control performance for each quarter sampled.	No exceptions noted.
CC1.2.4	Internal control performance metrics are provided to ISMS management on an annual basis. These metrics are documented in summary presentations for ISMS management review.	Inspected the internal control performance metrics documentation to determine that internal control performance metrics were provided to ISMS management and were documented in summary presentations for ISMS management review during the period.	No exceptions noted.
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The organizational structure, reporting lines, and authorities are defined in organizational charts, updated on an as needed basis, and communicated to employees via the company intranet.	Inspected the organizational chart on the company intranet to determine that the organizational structure, reporting lines, and authorities were defined in organizational charts, updated during the period, and communicated to employees via the company intranet.	No exceptions noted.
CC1.3.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC1.3.3	A security team that is composed of operations personnel and executive staff has been established to guide the company in managing security risks.	Inspected the information security policies and the most recent security team meeting calendar invitation, meeting minutes, and meeting attendees to determine that a security team that was composed of operations personnel and executive staff had been established to guide the company in managing security risks.	No exceptions noted.
CC1.3.4	Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.	Inspected the information security policy to determine that management had assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC1.4.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the employee hiring procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.3	Employees are required to complete security awareness training, upon hire and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training completion record for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training completion record for a sample of employees to determine that each employee sampled completed security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period.	No exceptions noted.
CC1.4.4	Management personnel monitor compliance with security awareness training requirements on an ongoing basis.	Inspected the security awareness training completion dashboard and an example reminder notification generated during the period to determine that management personnel monitored compliance with security awareness training requirements during the period.	No exceptions noted.
CC1.4.5	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inspected the online training portal to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.6	Employee performance reviews are conducted at least annually to evaluate employees against expected levels of performance.	Inspected the performance review documentation for a sample of employees to determine that a performance review was conducted to evaluate each employee sampled against expected levels of performance during the period.	No exceptions noted.
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the strategy meeting calendar invitation and the meeting slide deck for a sample of quarters during the period to determine that management held a company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives for each quarter sampled.	No exceptions noted.
CC1.5.2	Employee performance reviews are conducted at least annually to evaluate employees against expected levels of performance.	Inspected the performance review documentation for a sample of employees to determine that a performance review was conducted to evaluate each employee sampled against expected levels of performance during the period.	No exceptions noted.
CC1.5.3	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC1.5.4	An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the disciplinary action policy and procedure to determine that an employee sanction policy was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC1.5.5	A security team that is composed of operations personnel and executive staff has been established to guide the company in managing security risks.	Inspected the information security policies and the most recent security team meeting calendar invitation, meeting minutes, and meeting attendees to determine that a security team that was composed of operations personnel and executive staff had been established to guide the company in managing security risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.6	Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.	Inspected the information security policy to determine that management had assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.	No exceptions noted.
Communication and Information			
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Information system security and data classification policies are formally documented that identify information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information security and data classification policies and procedures to determine that information system security and data classification policies were formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
CC2.1.2	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.	No exceptions noted.
CC2.1.3	A third-party utility is configured to perform vulnerability scans on a daily basis. Security vulnerabilities above the tolerable threshold that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan configurations, an example vulnerability scan log generated during the period, and example remediation documentation during the period to determine that a third-party utility was configured to perform vulnerability scans on a daily basis and that security vulnerabilities above the tolerable threshold that were identified were triaged by IT security personnel and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.4	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities above the tolerable threshold that are detected are triaged by IT security personnel and monitored through resolution.	Inspected the most recent penetration test report and an example remediation ticket created during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities above the tolerable threshold that were detected were triaged by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CC2.1.5	Internal audits are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the most recent internal audit report and corrective action plan documentation to determine that internal audits were performed by management to gain assurance that controls were in place and operating effectively and that corrective actions were taken by management based on relevant findings and tracked to resolution during the period.	No exceptions noted.
CC2.1.6	The entity's IT security team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inspected an example security notification received during the period to determine that the entity's IT security team monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management during the period.	No exceptions noted.
CC2.1.7	A bug bounty program is in place to identify threats and assess their potential impact to the system. Reported vulnerabilities are reviewed by IT security personnel and monitored through resolution as needed.	Inspected the bug bounty program and an example bug resolved during the period to determine that a bug bounty program was in place to identify threats and assess their potential impact to the system and that reported vulnerabilities were reviewed by IT security personnel and monitored through resolution during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet.	Inspected the policies and procedures on the company intranet to determine that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems and that these policies and procedures were communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.2.2	Employees are required to complete security awareness training, upon hire and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training completion record for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	No exceptions noted.
		Inspected the security awareness training completion record for a sample of employees to determine that each employee sampled completed security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period.	No exceptions noted.
CC2.2.3	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employment position sampled.	No exceptions noted.
CC2.2.4	Documented escalation procedures for reporting incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident management policies and procedures to determine that documented escalation procedures for reporting incidents were provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	Management has assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.	Inspected the information security policy to determine that management had assigned the responsibility of the maintenance and enforcement of the entity's security, availability, and confidentiality policies and procedures to the CISO.	No exceptions noted.
CC2.2.6	An online whistleblower channel is accessible by internal and external users to report incidents, concerns, and complaints. Reports of concerns are reviewed by the HR team on an as needed basis.	Inquired of the lead manager of compliance services regarding the whistleblower channel to determine that an online whistleblower channel was accessible by internal and external users to report incidents, concerns, and complaints and that reports of concerns were reviewed by the HR team on an as needed basis.	No exceptions noted.
		Inspected the whistleblower policy and the whistleblower reporting documentation to determine that an online whistleblower channel was accessible by internal and external users to report incidents, concerns, and complaints.	No exceptions noted.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.	Inspected the company website to determine that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.
CC2.3.2	The entity's security, availability, and confidentiality commitments and the associated system requirements, including the security, contractual, and regulatory requirements, are documented in the SA.	Inspected the standard customer agreement templates to determine that the entity's security, availability, and confidentiality commitments and the associated system requirements, including the security, contractual, and regulatory requirements, were documented in the SA.	No exceptions noted.
CC2.3.3	Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.	Inspected the MSA for a sample of in-scope third-party service providers to determine that each in-scope third-party service provider sampled signed nondisclosure agreements of confidentiality and protection before information designated as confidential could be shared with third parties.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.4	The security, availability, and confidentiality commitments and obligations of vendors are documented and communicated via MSAs.	Inspected the MSA for a sample of in-scope vendors to determine that the security, availability, and confidentiality commitments and obligations were documented and communicated via MSAs for each vendor sampled.	No exceptions noted.
CC2.3.5	Documented escalation procedures for reporting incidents are provided to external users via the company website to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the customer support portal on the company website to determine that documented escalation procedures for reporting incidents were provided to external users via the company website to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.3.6	A web portal is accessible by external users to report security incidents, concerns, and complaints. Reports of concerns are reviewed by security personnel on an as needed basis.	Inquired of the lead compliance manager regarding the process for reviewing reports of concerns submitted by external users to determine that a web portal was accessible by external users to report security incidents, concerns, and complaints and that reports of concerns were reviewed by security personnel on an as needed basis.	No exceptions noted.
		Inspected the web portal on the company website and an example customer support ticket generated during the period to determine that a web portal was accessible by external users to report security incidents, concerns, and complaints and that reports of concerns were reviewed by security personnel during the period.	No exceptions noted.
CC2.3.7	System alerts, including planned changes to system components, planned outages, release notes, and known issues, are displayed on the external-facing website.	Inspected the status page on the company website to determine that system alerts, including planned changes to system components, planned outages, release notes, and known issues, were displayed on the external-facing website.	No exceptions noted.
CC2.3.8	A bug bounty program is in place to identify threats and assess their potential impact to the system. Reported vulnerabilities are reviewed by IT security personnel and monitored through resolution as needed.	Inspected the bug bounty program and an example bug resolved during the period to determine that a bug bounty program was in place to identify threats and assess their potential impact to the system and that reported vulnerabilities were reviewed by IT security personnel and monitored through resolution during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Assessment			
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to help ensure they align with the company's mission and are utilized as part of the annual risk assessment process.	Inspected the risk governance policy, the most recent risk assessment documentation, and the most recent risk review meeting to determine that management formally documented and reviewed the company's commitments and the operational, reporting, and compliance objectives to ensure they aligned with the company's mission and were utilized as part of the risk assessment process during the period.	No exceptions noted.
CC3.1.2	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the strategy meeting calendar invitation and the meeting slide deck for a sample of quarters during the period to determine that management held a company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives for each quarter sampled.	No exceptions noted.
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program documentation to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	A formal risk assessment is performed on an annual basis that considers the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed that considered the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.2.3	A third-party utility is configured to perform vulnerability scans on a daily basis. Security vulnerabilities above the tolerable threshold that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan configurations, an example vulnerability scan log generated during the period, and example remediation documentation during the period to determine that a third-party utility was configured to perform vulnerability scans on a daily basis and that security vulnerabilities above the tolerable threshold that were identified were triaged by IT security personnel and monitored through resolution.	No exceptions noted.
CC3.2.4	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities above the tolerable threshold that are detected are triaged by IT security personnel and monitored through resolution.	Inspected the most recent penetration test report and an example remediation ticket created during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities above the tolerable threshold that were detected were triaged by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program documentation to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3.2	A formal risk assessment is performed on an annual basis that considers the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed that considered the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program documentation to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.4.2	A formal risk assessment is performed on an annual basis that considers the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed that considered the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.4.3	Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process.	Inspected the most recent risk assessment documentation to determine that management identified and assessed changes that could significantly impact the system of internal control as part of the risk assessment process during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Monitoring Activities			
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Internal audits are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the most recent internal audit report and corrective action plan documentation to determine that internal audits were performed by management to gain assurance that controls were in place and operating effectively and that corrective actions were taken by management based on relevant findings and tracked to resolution during the period.	No exceptions noted.
CC4.1.2	A third-party utility is configured to perform vulnerability scans on a daily basis. Security vulnerabilities above the tolerable threshold that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan configurations, an example vulnerability scan log generated during the period, and example remediation documentation during the period to determine that a third-party utility was configured to perform vulnerability scans on a daily basis and that security vulnerabilities above the tolerable threshold that were identified were triaged by IT security personnel and monitored through resolution.	No exceptions noted.
CC4.1.3	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities above the tolerable threshold that are detected are triaged by IT security personnel and monitored through resolution.	Inspected the most recent penetration test report and an example remediation ticket created during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities above the tolerable threshold that were detected were triaged by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CC4.1.4	The security team reviews changes to critical vendors along with their completed audit reports on an annual basis and determines the impact of any changes in relation to the organization's objectives and the impact to internal control.	Inspected the most recent vendor assessment documentation for a sample of critical vendors to determine that the security team reviewed vendors along with their completed audit reports and determined the impact of any changes in relation to the organization's objectives and the impact to internal control during the period for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Internal audits are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the most recent internal audit report and corrective action plan documentation to determine that internal audits were performed by management to gain assurance that controls were in place and operating effectively and that corrective actions were taken by management based on relevant findings and tracked to resolution during the period.	No exceptions noted.
CC4.2.2	Internal control performance metrics are provided to ISMS management on an annual basis. These metrics are documented in summary presentations for ISMS management review.	Inspected the internal control performance metrics documentation to determine that internal control performance metrics were provided to ISMS management and were documented in summary presentations for ISMS management review during the period.	No exceptions noted.
CC4.2.3	A security team that is composed of operations personnel and executive staff has been established to guide the company in managing security risks.	Inspected the information security policies and the most recent security team meeting calendar invitation, meeting minutes, and meeting attendees to determine that a security team that was composed of operations personnel and executive staff had been established to guide the company in managing security risks.	No exceptions noted.
CC4.2.4	Management holds a quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the strategy meeting calendar invitation and the meeting slide deck for a sample of quarters during the period to determine that management held a company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Activities			
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program documentation to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.2	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within risk treatment plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment documentation to determine that assigned risk owners selected and developed control activities to mitigate the risks identified as part of the risk assessment process and that the control activities were documented within risk treatment plans that were created by the risk owners for risks above the tolerable threshold during the period.	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.			
CC5.2.1	Assigned risk owners select and develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment documentation to determine that assigned risk owners selected and developed control activities over technology to support the achievement of objectives as an output from the risk assessment and that the control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet.	Inspected the policies and procedures on the company intranet to determine that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems and that these policies and procedures were communicated to internal personnel via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.2	Information system security and data classification policies are formally documented that identify information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	Inspected the information security and data classification policies and procedures to determine that information system security and data classification policies were formally documented that identified information required to support the functioning of internal control and achievement of objectives and associated protection and access rights.	No exceptions noted.
CC5.3.3	An employee sanction policy is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the disciplinary action policy and procedure to determine that an employee sanction policy was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
Logical and Physical Access Controls			
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.			
CC6.1.1	The security team has formally documented standard build procedures for installation and maintenance of production systems.	Inspected the standard build procedures to determine that the security team had formally documented standard build procedures for installation and maintenance of production systems.	No exceptions noted.
CC6.1.2	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements, and MFA or SSH authentication, as applicable.	<p>Inspected the user account listing and authentication configurations for a sample of in-scope systems to determine that the following sampled in-scope systems were configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements, and MFA or SSH authentication, as applicable:</p> <ul style="list-style-type: none"> • Identity management service • Cloud infrastructure consoles • Infrastructure access platform • Production servers • Production containers • Production databases • Password management tool 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the in-scope systems.	Inspected the administrator user account listing for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the following sampled in-scope systems: <ul style="list-style-type: none"> • Identity management service • Cloud infrastructure consoles • Infrastructure access platform • Production servers • Production containers • Production databases • Password management tool 	No exceptions noted.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listing for a sample of in-scope systems with the assistance of the director of product security to determine that administrative access privileges to the following sampled in-scope systems were restricted to user accounts accessible by authorized personnel: <ul style="list-style-type: none"> • Identity management service • Cloud infrastructure consoles • Infrastructure access platform • Production servers • Production containers • Production databases • Password management tool 	No exceptions noted.
CC6.1.5	Confidential data is stored in an encrypted format.	Inspected the encryption configurations for a sample of databases to determine that confidential data was stored in an encrypted format for each database sampled.	No exceptions noted.
CC6.1.6	The production network is logically segmented to help ensure that confidential data is isolated from other unrelated networks.	Inspected the production environment network configurations to determine that the production network was logically segmented to ensure that confidential data was isolated from other unrelated networks.	No exceptions noted.
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.02	MongoDB and Snowflake are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.		
CSOC.03	Google and Snowflake are responsible for ensuring data within GCP and Snowflake are stored in an encrypted at rest format.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CSOC.04	AWS, Google, MongoDB, and Snowflake are responsible for ensuring access to server-side encryption keys is restricted to authorized personnel.		
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Production system access requests are documented in an automated ticketing system and require the approval of a manager prior to access being granted.	Inspected the production system access request ticket for a sample of user accounts provisioned during the period to determine that each user account sampled was documented in a production system access request in the automated ticketing system and received the approval of a manager prior to access being granted.	No exceptions noted.
CC6.2.2	A termination ticket is completed, and system access is revoked as a component of the employee termination process.	Inspected the termination ticket and the user account listing for a sample of in-scope systems and employees terminated during the period to determine that a termination ticket was completed, and system access was revoked as a component of the employee termination process for each employee and system sampled: <ul style="list-style-type: none">• Identity management service• Cloud infrastructure consoles• Infrastructure access platform• Production servers• Production containers• Production databases• Password management tool	No exceptions noted.
CC6.2.3	User access reviews, including privileged users, are performed by management quarterly to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews, including privileged users, were performed by management to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved for each quarter sampled.	No exceptions noted.
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.02	MongoDB and Snowflake are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Production system access requests are documented in an automated ticketing system and require the approval of a manager prior to access being granted.	Inspected the production system access request ticket for a sample of user accounts provisioned during the period to determine that each user account sampled was documented in a production system access request in the automated ticketing system and received the approval of a manager prior to access being granted.	No exceptions noted.
CC6.3.2	A termination ticket is completed, and system access is revoked as a component of the employee termination process.	Inspected the termination ticket and the user account listing for a sample of in-scope systems and employees terminated during the period to determine that a termination ticket was completed, and system access was revoked as a component of the employee termination process for each employee and system sampled: <ul style="list-style-type: none"> • Identity management service • Cloud infrastructure consoles • Infrastructure access platform • Production servers • Production containers • Production databases • Password management tool 	No exceptions noted.
CC6.3.3	User access reviews, including privileged users, are performed by management quarterly to help ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews, including privileged users, were performed by management to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.4	Predefined security groups are utilized to assign role-based access privileges and restrict access to data to the in-scope systems.	Inspected the administrator user account listing for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and restrict access to data to the following sampled in-scope systems: <ul style="list-style-type: none">• Identity management service• Cloud infrastructure consoles• Infrastructure access platform• Production servers• Production containers• Production databases• Password management tool	No exceptions noted.
CC6.3.5	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listing for a sample of in-scope systems with the assistance of the director of product security to determine that administrative access privileges to the following sampled in-scope systems were restricted to user accounts accessible by authorized personnel: <ul style="list-style-type: none">• Identity management service• Cloud infrastructure consoles• Infrastructure access platform• Production servers• Production containers• Production databases• Password management tool	No exceptions noted.
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.02	MongoDB and Snowflake are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.		
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CSOC.05	AWS and Google are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
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.			
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.05	AWS and Google are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Security groups are in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the network security group configurations to determine that security groups were in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that was not explicitly authorized by a rule.	No exceptions noted.
CC6.6.2	A WAF is utilized to monitor and analyze web application events for possible or actual security breaches, and filter, monitor, and block inbound and outbound traffic from the Internet.	Inspected the WAF ruleset configurations to determine that a WAF was utilized to monitor and analyze web application events for possible or actual security breaches, and filter, monitor, and block inbound and outbound traffic from the Internet.	No exceptions noted.
CC6.6.3	A HIDS is utilized to analyze and report network events and to block suspected or actual network security breaches. Notifications are sent to IT security personnel to analyze and respond to events.	Inspected the HIDS configurations and an example alert generated during the period to determine that a HIDS was utilized to analyze and report network events and to block suspected or actual network security breaches and that notifications were sent to IT security personnel to analyze and respond to events during the period.	No exceptions noted.
CC6.6.4	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS certificate to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.6.5	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.6	A third-party utility is configured to perform vulnerability scans on a daily basis. Security vulnerabilities above the tolerable threshold that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan configurations, an example vulnerability scan log generated during the period, and example remediation documentation during the period to determine that a third-party utility was configured to perform vulnerability scans on a daily basis and that security vulnerabilities above the tolerable threshold that were identified were triaged by IT security personnel and monitored through resolution.	No exceptions noted.
CC6.6.7	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities above the tolerable threshold that are detected are triaged by IT security personnel and monitored through resolution.	Inspected the most recent penetration test report and an example remediation ticket created during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities above the tolerable threshold that were detected were triaged by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.02	MongoDB and Snowflake are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.		
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Documented policies and procedures are in place to guide personnel in the handling and encryption of stored data and data in transit.	Inspected the cryptography policies and procedures to determine that documented policies and procedures were in place to guide personnel in the handling and encryption of stored data and data in transit.	No exceptions noted.
CC6.7.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS certificate to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.7.3	A HIDS is utilized to analyze and report network events and to block suspected or actual network security breaches. Notifications are sent to IT security personnel to analyze and respond to events.	Inspected the HIDS configurations and an example alert generated during the period to determine that a HIDS was utilized to analyze and report network events and to block suspected or actual network security breaches and that notifications were sent to IT security personnel to analyze and respond to events during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.4	MDM software is configured to encrypt the hard drives of Snyk-owned workstations.	Inspected the MDM configurations and endpoint listing to determine that MDM software was configured to encrypt the hard drives of Snyk-owned workstations.	No exceptions noted.
CSOC.06	AWS and Google are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the Snyk systems reside.		
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	EDR software is configured to install and manage the enterprise antivirus software on Snyk-owned workstations and enforces behavior-based prevention policies to prevent the introduction of unauthorized or malicious software. The EDR software is configured to be automatically updated on a continuous basis.	Inspected the EDR software configurations and endpoint listing to determine that EDR software was configured to install and manage the enterprise antivirus software on Snyk-owned workstations, enforced behavior-based prevention policies to prevent the introduction of unauthorized or malicious software, and that the EDR software was configured to be automatically updated on a continuous basis.	No exceptions noted.
CC6.8.2	The ability to install applications or software is restricted to authorized engineering personnel.	Inspected the listing of user accounts with access to production systems with the assistance of the director of product security to determine that the ability to install applications or software was restricted to authorized engineering personnel.	No exceptions noted.
System Operations			
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The security team has formally documented standard build procedures for installation and maintenance of production systems.	Inspected the standard build procedures to determine that the security team had formally documented standard build procedures for installation and maintenance of production systems.	No exceptions noted.
CC7.1.2	A third-party utility is configured to perform vulnerability scans on a daily basis. Security vulnerabilities above the tolerable threshold that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan configurations, an example vulnerability scan log generated during the period, and example remediation documentation during the period to determine that a third-party utility was configured to perform vulnerability scans on a daily basis and that security vulnerabilities above the tolerable threshold that were identified were triaged by IT security personnel and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.3	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities above the tolerable threshold that are detected are triaged by IT security personnel and monitored through resolution.	Inspected the most recent penetration test report and an example remediation ticket created during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities above the tolerable threshold that were detected were triaged by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CC7.1.4	The automated deployment tool is configured to notify operations personnel via the team collaboration tool when deployments to production occur.	Inspected the automated deployment tool alerting configurations and an example alert generated during the period to determine that the automated deployment tool was configured to notify operations personnel via the team collaboration tool when deployments to production occurred.	No exceptions noted.
CC7.1.5	A bug bounty program is in place to identify threats and assess their potential impact to the system. Reported vulnerabilities are reviewed by IT security personnel and monitored through resolution as needed.	Inspected the bug bounty program and an example bug resolved during the period to determine that a bug bounty program was in place to identify threats and assess their potential impact to the system and that reported vulnerabilities were reviewed by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, and resource utilization, and to alert IT security personnel upon detection of unusual system activity or service requests.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.2	A third-party utility is configured to perform vulnerability scans on a daily basis. Security vulnerabilities above the tolerable threshold that are identified are triaged by IT security personnel and monitored through resolution.	Inspected the vulnerability scan configurations, an example vulnerability scan log generated during the period, and example remediation documentation during the period to determine that a third-party utility was configured to perform vulnerability scans on a daily basis and that security vulnerabilities above the tolerable threshold that were identified were triaged by IT security personnel and monitored through resolution.	No exceptions noted.
CC7.2.3	Penetration testing is performed by a third-party vendor on an annual basis. Security vulnerabilities above the tolerable threshold that are detected are triaged by IT security personnel and monitored through resolution.	Inspected the most recent penetration test report and an example remediation ticket created during the period to determine that penetration testing was performed by a third-party vendor and that security vulnerabilities above the tolerable threshold that were detected were triaged by IT security personnel and monitored through resolution during the period.	No exceptions noted.
CC7.2.4	A HIDS is utilized to analyze and report network events and to block suspected or actual network security breaches. Notifications are sent to IT security personnel to analyze and respond to events.	Inspected the HIDS configurations and an example alert generated during the period to determine that a HIDS was utilized to analyze and report network events and to block suspected or actual network security breaches and that notifications were sent to IT security personnel to analyze and respond to events during the period.	No exceptions noted.
CSOC.07	AWS and Google are responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.08	MongoDB and Snowflake are responsible for monitoring the logical access control systems for the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.		
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Security incident response policies and procedures are documented and provide guidance to internal personnel for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated via the company intranet.	Inspected the security incident response policies and procedures documentation to determine that security incident response policies and procedures were documented and provided guidance to internal personnel for detecting, responding to, and recovering from security events and incidents and that the policies and procedures were communicated via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.2	Security team meetings are held monthly to help ensure the alignment of information security and business objectives, discuss the effect of identified security vulnerabilities on the ability to meet business objectives, respond to security incidents, and identify corrective measures.	Inspected the security team meeting documentation for a sample of months during the period to determine that security team meetings were held to ensure the alignment of information security and business objectives, discussed the effect of identified security vulnerabilities on the ability to meet business objectives, responded to security incidents, and identified corrective measures for each month sampled.	No exceptions noted.
CC7.3.3	Security events are logged, tracked, resolved, and communicated to affected parties, as necessary, in alignment with security incident response policies and procedures.	Inspected the security incident documentation for a sample of security incidents closed during the period to determine that security events were logged, tracked, resolved, and communicated to affected parties, as necessary, in alignment with security incident response policies and procedures for each security incident sampled.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Security incident response policies and procedures are documented and provide guidance to internal personnel for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated via the company intranet.	Inspected the security incident response policies and procedures documentation to determine that security incident response policies and procedures were documented and provided guidance to internal personnel for detecting, responding to, and recovering from security events and incidents and that the policies and procedures were communicated via the company intranet.	No exceptions noted.
CC7.4.2	Security team meetings are held monthly to help ensure the alignment of information security and business objectives, discuss the effect of identified security vulnerabilities on the ability to meet business objectives, respond to security incidents, and identify corrective measures.	Inspected the security team meeting documentation for a sample of months during the period to determine that security team meetings were held to ensure the alignment of information security and business objectives, discussed the effect of identified security vulnerabilities on the ability to meet business objectives, responded to security incidents, and identified corrective measures for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	Security events are logged, tracked, resolved, and communicated to affected parties, as necessary, in alignment with security incident response policies and procedures.	Inspected the security incident documentation for a sample of security incidents closed during the period to determine that security events were logged, tracked, resolved, and communicated to affected parties, as necessary, in alignment with security incident response policies and procedures for each security incident sampled.	No exceptions noted.
CC7.4.4	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.	Inspected the most recent incident response plan test to determine that the incident response plan was tested to assess the effectiveness of the incident response program during the period.	No exceptions noted.
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Security incident response policies and procedures are documented and provide guidance to internal personnel for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated via the company intranet.	Inspected the security incident response policies and procedures documentation to determine that security incident response policies and procedures were documented and provided guidance to internal personnel for detecting, responding to, and recovering from security events and incidents and that the policies and procedures were communicated via the company intranet.	No exceptions noted.
CC7.5.2	Security team meetings are held monthly to help ensure the alignment of information security and business objectives, discuss the effect of identified security vulnerabilities on the ability to meet business objectives, respond to security incidents, and identify corrective measures.	Inspected the security team meeting documentation for a sample of months during the period to determine that security team meetings were held to ensure the alignment of information security and business objectives, discussed the effect of identified security vulnerabilities on the ability to meet business objectives, responded to security incidents, and identified corrective measures for each month sampled.	No exceptions noted.
CC7.5.3	Security events are logged, tracked, resolved, and communicated to affected parties, as necessary, in alignment with security incident response policies and procedures.	Inspected the security incident documentation for a sample of security incidents closed during the period to determine that security events were logged, tracked, resolved, and communicated to affected parties, as necessary, in alignment with security incident response policies and procedures for each security incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.4	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.	Inspected the most recent incident response plan test to determine that the incident response plan was tested to assess the effectiveness of the incident response program during the period.	No exceptions noted.
Change Management			
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change management policies and procedures are in place to guide personnel in the request, documentation, peer review, testing, and approval of changes.	Inspected the change management policies and procedures to determine that change management policies and procedures were in place to guide personnel in the request, documentation, peer review, testing, and approval of changes.	No exceptions noted.
CC8.1.2	Changes made to in-scope systems are authorized, tested, and approved prior to implementation.	Inspected the change ticket documentation for a sample of application and infrastructure changes implemented during the period to determine that each change sampled was authorized, tested, and approved prior to implementation.	No exceptions noted.
CC8.1.3	The production environment is logically segmented from development and test environments.	Inspected the network segmentation configurations to determine that the production environment was logically segmented from development and test environments.	No exceptions noted.
CC8.1.4	The version control software is configured to restrict users from merging code without peer approval, thus preventing any user from both developing and implementing code to the production environment.	Inspected the branch protection rule configurations for a sample of in-scope repositories to determine that the version control software was configured to restrict users from merging code without peer approval, thus preventing any user from both developing and implementing code to the production environment for each in-scope repository sampled.	No exceptions noted.
CC8.1.5	Write access to the version control software is restricted to user accounts accessible by authorized personnel.	Inspected the version control software administrator user account listing and the listing of user accounts with write access with the assistance of the director of product security for a sample of in-scope repositories to determine that write access to the version control software was restricted to user accounts accessible by authorized personnel for each repository sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.6	Access privileges to deploy changes into the production environment are restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with access to deploy changes into the production environment with the assistance of the director of product security to determine that access privileges to deploy changes into the production environment were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.7	Administrative access privileges within the version control and deployment system are restricted to user accounts accessible by authorized personnel.	Inspected the version control and deployment system administrator user account listings with the assistance of the lead compliance manager to determine that administrative access privileges within the version control and deployment system were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.8	The automated deployment tool is configured to notify operations personnel via the team collaboration tool when deployments to production occur.	Inspected the automated deployment tool alerting configurations and an example alert generated during the period to determine that the automated deployment tool was configured to notify operations personnel via the team collaboration tool when deployments to production occurred.	No exceptions noted.
CC8.1.9	Production customer data is not utilized for development or testing in non-production environments.	Inspected example staging environment data generated during the period to determine that production customer data was not utilized for development or testing in non-production environments.	No exceptions noted.
Risk Mitigation			
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program documentation to determine that a documented risk management program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	A formal risk assessment is performed on an annual basis that considers the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed that considered the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC9.1.3	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and are reviewed, updated, and approved on an annual basis.	Inspected the disaster recovery plans to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and were reviewed, updated, and approved during the period.	No exceptions noted.
CC9.1.4	Disaster recovery plans are tested on an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the most recent disaster recovery plan test results to determine that the disaster recovery plans were tested to ensure the production environment could be recovered in the event of a disaster during the period.	No exceptions noted.
CC9.1.5	The company maintains cybersecurity insurance to mitigate the financial impact of a business disruption.	Inspected the active certificate of liability insurance during the period to determine that the company maintained cybersecurity insurance to mitigate the financial impact of a business disruption.	No exceptions noted.
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Documented vendor management policies and procedures are in place to guide personnel in assessing and managing risks associated with third parties.	Inspected the vendor management policies and procedures to determine that documented vendor management policies and procedures were in place to guide personnel in assessing and managing risks associated with third parties.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	The security team reviews changes to critical vendors along with their completed audit reports on an annual basis and determines the impact of any changes in relation to the organization's objectives and the impact to internal control.	Inspected the most recent vendor assessment documentation for a sample of critical vendors to determine that the security team reviewed vendors along with their completed audit reports and determined the impact of any changes in relation to the organization's objectives and the impact to internal control during the period for each vendor sampled.	No exceptions noted.
CC9.2.3	A formal risk assessment is performed on an annual basis that considers the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed that considered the identification and assessment of internal and external risks relating to company objectives, including risks arising from potential business disruptions, vendors, the impact of changes to the system, and the potential for fraud, and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC9.2.4	Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.	Inspected the MSA for a sample of in-scope third-party service providers to determine that each in-scope third-party service provider sampled signed nondisclosure agreements of confidentiality and protection before information designated as confidential could be shared with third parties.	No exceptions noted.
CC9.2.5	The security, availability, and confidentiality commitments and obligations of vendors are documented and communicated via MSAs.	Inspected the MSA for a sample of in-scope vendors to determine that the security, availability, and confidentiality commitments and obligations were documented and communicated via MSAs for each vendor sampled.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
A1.1.1	Monitoring tools are used to continuously monitor security events, latency, network performance, and virtual server performance, and to send alerts to IT security personnel when predefined thresholds are exceeded.	Inspected the monitoring tool configurations and example alerts generated during the period to determine that monitoring tools were used to continuously monitor security events, latency, network performance, and virtual server performance, and to send alerts to IT security personnel when predefined thresholds were exceeded.	No exceptions noted.
CSOC.09	AWS, Google, MongoDB, and Snowflake are responsible for monitoring the capacity demand and ensuring capacity resources are available and functioning to meet Snyk’s availability commitments and requirements.		
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Formal procedures are documented to guide personnel in back up processes and recovering data.	Inspected the backup policies and procedures to determine that formal procedures were documented to guide personnel in back up processes and recovering data.	No exceptions noted.
A1.2.2	Production data is replicated across separate availability zones.	Inspected the replication configurations for a sample of production databases to determine that production data was replicated across separate availability zones for each database sampled.	No exceptions noted.
A1.2.3	Automated backup systems are in place to perform database backups at least daily.	Inspected the backup configurations for a sample of production databases and an example backup log generated during the period to determine that automated backup systems were in place to perform backups at least daily for each database sampled.	No exceptions noted.
A1.2.4	Automated backup systems are configured to retain backups of customer data in accordance with the backup policy.	Inspected the backup policy and the backup retention configurations for a sample of production databases to determine that automated backup systems were configured to retain backups of customer data in accordance with the backup policy for each database sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.5	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and are reviewed, updated, and approved on an annual basis.	Inspected the disaster recovery plans to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event and were reviewed, updated, and approved during the period.	No exceptions noted.
CSOC.10	AWS and Google are responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing a monitoring application to monitor for environmental events.		
CSOC.11	Snowflake is responsible for performing scheduled backups and replication of Snowflake databases to multiple diverse locations at predefined times.		
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Disaster recovery plans are tested on an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the most recent disaster recovery plan test results to determine that the disaster recovery plans were tested to ensure the production environment could be recovered in the event of a disaster during the period.	No exceptions noted.
A1.3.2	Engineering personnel perform backup data restores on an annual basis to help ensure that system components can be recovered from system backups.	Inspected the most recent backup data restore documentation to determine that engineering personnel performed backup data restores to ensure that system components could be recovered from system backups during the period.	No exceptions noted.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Documented data classification policies are in place to help ensure that confidential data is properly maintained, restricted to authorized personnel, and prohibited from being used or stored outside of company-approved methods.	Inspected the data classification policy to determine that documented data classification policies were in place to ensure that confidential data was properly maintained, restricted to authorized personnel, and prohibited from being used or stored outside of company-approved methods.	No exceptions noted.
C1.1.2	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of company and customer data.	Inspected the data retention and disposal policies and procedures to determine that formal data retention and disposal procedures were documented to guide the secure retention and disposal of company and customer data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1.3	Production customer data is not utilized for development or testing in non-production environments.	Inspected example staging environment data generated during the period to determine that production customer data was not utilized for development or testing in non-production environments.	No exceptions noted.
C1.1.4	Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties.	Inspected the MSA for a sample of in-scope third-party service providers to determine that each in-scope third-party service provider sampled signed nondisclosure agreements of confidentiality and protection before information designated as confidential could be shared with third parties.	No exceptions noted.
C1.1.5	Confidential data is stored in an encrypted format.	Inspected the encryption configurations for a sample of databases to determine that confidential data was stored in an encrypted format for each database sampled.	No exceptions noted.
C1.1.6	Backups are stored in an encrypted format.	Inspected the backup encryption configurations for a sample of production databases to determine that each database sampled was configured to store backups in an encrypted format.	No exceptions noted.
C1.1.7	Administrative access privileges within the version control and deployment system are restricted to user accounts accessible by authorized personnel.	Inspected the version control and deployment system administrator user account listings with the assistance of the lead compliance manager to determine that administrative access privileges within the version control and deployment system were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CSOC.01	AWS and Google are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Snyk systems reside.		
CSOC.02	MongoDB and Snowflake are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their DBaaS services where the Snyk systems reside.		
CSOC.03	Google and Snowflake are responsible for ensuring data within GCP and Snowflake are stored in an encrypted at rest format.		
CSOC.04	AWS, Google, MongoDB, and Snowflake are responsible for ensuring access to server-side encryption keys is restricted to authorized personnel.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of company and customer data.	Inspected the data retention and disposal policies and procedures to determine that formal data retention and disposal procedures were documented to guide the secure retention and disposal of company and customer data.	No exceptions noted.
C1.2.2	Snyk has established a data retention standard to retain backup data for current customers. Snyk enforces the standard such that customer data backups are retained for up to 90 days after which they are deleted from the backup location.	Inspected the data retention standard, backup data retention configurations, and data retention logs for a sample of production databases to determine that Snyk had established a data retention standard to retain backup data for current customers and that Snyk enforced the standard such that customer data backups were retained for up to 90 days after which they were deleted from the backup location.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY SNYK

SNYK API & WEB

Snyk API & Web allows customers to discover and test the security of their APIs and web apps, even those whose code was generated by AI, and get detailed instructions on how to fix the findings. Please note: this product offering is covered in a separate report. Refer to the Snyk API & Web SOC 2 Type II report for information pertaining to this product offering.