DigitalOcean

System and Organization Controls 2 Report

Description of DigitalOcean's Cloud Infrastructure Platform
throughout the period January 1, 2025 - December 31, 2025
with Independent Service Auditor's Report



This report is intended solely for use by the management of DigitalOcean, LLC, user entities of DigitalOcean, LLC's services, and other parties who have sufficient knowledge and understanding of DigitalOcean, LLC'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 24

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To DigitalOcean, LLC:

Scope

We have examined DigitalOcean, LLC's ("DigitalOcean" or the "service organization") accompanying description of its Cloud Infrastructure Platform system, in Section 3, throughout the period January 1, 2025, to December 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 January 1, 2025, to December 31, 2025, to provide reasonable assurance that DigitalOcean's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("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).*

DigitalOcean uses various subservice organizations for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DigitalOcean, to achieve DigitalOcean's service commitments and system requirements based on the applicable trust services criteria. The description presents DigitalOcean's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DigitalOcean'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.

Service Organization's Responsibilities

DigitalOcean 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 DigitalOcean's service commitments and system requirements were achieved. DigitalOcean has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. DigitalOcean 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 DigitalOcean's Cloud Infrastructure Platform system that was designed and implemented throughout the period January 1, 2025, to December 31, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that DigitalOcean'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 DigitalOcean's controls throughout that period; and

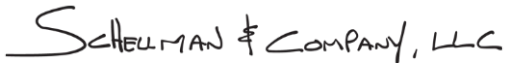
- the controls stated in the description operated effectively throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that DigitalOcean's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of DigitalOcean'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 DigitalOcean, user entities of DigitalOcean's Cloud Infrastructure Platform system during some or all of the period of January 1, 2025, to December 31, 2025, business partners of DigitalOcean subject to risks arising from interactions with the Cloud Infrastructure 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.



Charlotte, North Carolina
February 3, 2026

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of DigitalOcean's Cloud Infrastructure Platform system, in Section 3, throughout the period January 1, 2025, to December 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 Cloud Infrastructure Platform system that may be useful when assessing the risks arising from interactions with DigitalOcean's system, particularly information about system controls that DigitalOcean 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 and availability ("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)*.

DigitalOcean uses various subservice organizations for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DigitalOcean, to achieve DigitalOcean's service commitments and system requirements based on the applicable trust services criteria. The description presents DigitalOcean's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DigitalOcean'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 DigitalOcean's Cloud Infrastructure Platform system that was designed and implemented throughout the period January 1, 2025, to December 31, 2025, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that DigitalOcean'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 DigitalOcean's controls throughout that period; and
- the controls stated in the description operated effectively throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that DigitalOcean'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 DigitalOcean's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

DigitalOcean, founded in 2012, provides cloud services to deploy, manage, and scale applications with the intent of removing infrastructure friction and providing predictability. The DigitalOcean cloud services provide its customers with a user interface and application programming interfaces ("APIs"), a robust set of features, tutorials, and a library of open-source resources.

Description of Services Provided

DigitalOcean's Cloud Infrastructure Platform allows users to build, deploy, and scale applications while leveraging the services of DigitalOcean for the handling, provisioning, and managing of infrastructure, databases, and operating systems. Furthermore, DigitalOcean's products and services are virtualized to help ensure it has the ability to scale to meet demand.

DigitalOcean provides Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Function as a service ("FaaS") offerings. The various products for each of DigitalOcean's IaaS, PaaS, and FaaS offerings are described below:

IaaS Offerings

Droplets

Droplets are Linux-based virtual machines ("VMs") that run on top of virtualized hardware. Each Droplet created is a new server customers can use, either standalone or as part of a larger, cloud-based infrastructure.

GPU Droplets

GPU Droplets are Linux-based VMs that run on top of virtualized hardware. GPU Droplets offer on-demand access to high-powered GPUs to help customers train AI models, process large datasets, and handle complex neural networks.

Volumes Block Storage

Volumes block storage are network-based block devices that provide additional data storage for Droplets. Droplets are moveable and can be resized at any time.

Spaces

Spaces is an S3-compatible object storage service that allows for storage of large amounts of data. Each Space is a bucket to store and serve files. The free, built-in Spaces content delivery network minimizes page load times, improves performance, and reduces bandwidth and infrastructure costs.

Network File Storage

Network file storage is a fully managed file storage solution for high-performance and collaborative workloads. The product allows multiple servers or container clusters to access the same shared data simultaneously over a private network.

PaaS Offerings

Kubernetes

DigitalOcean Kubernetes ("DOKS") is a managed Kubernetes service that allows for the deployment of Kubernetes clusters without the complexities of handling the control plane and containerized infrastructure. Clusters are compatible with standard Kubernetes toolchains and integrate natively with DigitalOcean load balancers and volumes block storage.

Managed Databases

Managed Databases are a fully managed database cluster service. Using managed databases is an alternative to installing, configuring, maintaining, and securing databases manually.

App Platform

App Platform allows developers to publish code directly to DigitalOcean servers without having to manage the underlying infrastructure.

App Platform can either automatically analyze and build code from your GitHub, GitLab or public Git repositories and publish applications to the cloud or publish a container image already uploaded to DigitalOcean Container Registry or Docker Hub. It also has lifecycle management features, vertical and horizontal scaling, push-to-deploy support, introspection and monitoring features, built-in database management and integration.

Gradient AI Platform

The gradient AI platform allows developers to develop and deploy production ready AI agents and applications. The Platform integrates serverless interference for foundation models with specialized tools for Retrieval Augmented Generation ("RAG"), including managed knowledge bases, automated data indexing, and built-in guardrails for security and safety.

Container Registry

The DigitalOcean Container Registry ("DOCR") offers the security of a private Docker image registry, with extra tool support that enables integration with Docker environments and DOKS clusters. These registries are private and co-located in the data centers where DOKS clusters are operated, to help ensure secure, stable, and performant rollout of images to your clusters.

FaaS Offerings

Functions

Functions are blocks of code configured to run on demand without the need to manage infrastructure. Functions are designed to allow end users to deploy code that can perform the same tasks as a traditional API without the requirement of configuring a server to manage the requests. Each function that an end user deploys is assigned a unique URL, which the end user can use to anonymously test the function. End users can further invoke their functions and inspect the logs and results directly from their terminal.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

DigitalOcean designs its processes and procedures related to the Cloud Infrastructure Platform system to meet its business objectives for the DigitalOcean cloud offerings. Those objectives are based on service commitments that the organization makes to user entities, the laws and regulations that govern the provisioning of its cloud offerings, and the financial, operational, and compliance requirements that the organization has established for the services. The Cloud Infrastructure Platform system is subject to the relevant regulatory, industry, and data security requirements in which DigitalOcean operates.

The security and availability commitments to user entities are documented and communicated to customers in service agreements and company policies. The principal security commitments are standardized and include, but are not limited to, the following:

- Maintain written information security policies that define security controls based on DigitalOcean's assessment of risk to personal data that it processes and its information systems.
- Employ security technologies and measures designed to protect information from unauthorized access, use, or disclosure of DigitalOcean management network and assets.
- Encrypt customer data in transit between the DigitalOcean's management network and infrastructure.

- Conduct a variety of regular internal and external audits that are inclusive of security operations.
- Grant access to DigitalOcean assets based on least-privileges principles.
- Utilize logging and monitoring tools to analyze service, user, and security events.
- Maintain infrastructure within multiple availability zones in geographic regions physically separated from one another of DigitalOcean management network and assets.
- Maintain monitoring mechanisms over infrastructure to check server performance, data, traffic, and load capacity and to detect and route issues experienced by hosts in real time and employ orchestration tooling that has the ability to regenerate hosts.

Additionally, DigitalOcean provides service level agreements ("SLAs") for the following products, which display its commitment to deliver a high level of availability for customers products, including Droplets, Volumes Block Storage, and Kubernetes Control Plane, among others.

- IaaS
    - Droplets: The DigitalOcean Droplet service provides a 99.99% uptime SLA per month.
    - GPU Droplets: The DigitalOcean GPU Droplet provides a 99% uptime SLA per month
    - Block Storage: The DigitalOcean Volumes Block Storage service provides 99.9% uptime SLA per month.
- PaaS
    - Kubernetes: The DOKS service provides 99.95% uptime SLA per month for the control plane when high availability ("HA") is enabled for such clusters.
    - Managed Databases: The DigitalOcean Managed Databases provides a 99.95% uptime SLA for configurations with standby nodes and a 99.5% uptime SLA for configurations without standby nodes.
    - AppPlatform: The DigitalOcean AppPlatform provides a 99.95% uptime SLA for each App Component Instance ("ACI") per month.

DigitalOcean establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements are communicated in DigitalOcean's information security policies, service agreements, and training documentation and include, but are not limited to, the following:

- Information security policies are documented and made available to workforce members.
- Enforcing authentication requirements for in-scope systems.
- Requiring formal approval by a workforce member's direct supervisor or software owner for access provisioning requests and revoking access to in-scope systems upon termination of personnel.
- Encrypting web communication sessions using the TLS encryption protocol.
- Collecting data from in-scope systems and production hosts to analyze system performance, resource utilization, and potential security vulnerabilities.
- Utilizing a vulnerability scanning tool and bug bounty program to identify and mitigate system vulnerabilities.
- Penetration tests are performed by third-party vendors annually to identify threats from sources outside the boundaries of the system and assess their potential impact to the system.

In accordance with DigitalOcean's 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 all system users, 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 supporting the DigitalOcean Cloud Infrastructure Platform production systems are hosted from multiple regional facilities ("regions") that reside in facilities managed by various colocation data centers. Available regions are located in the United States, United Kingdom, Singapore, Netherlands, Canada, India, Australia, and Germany. DigitalOcean offers an IaaS platform for software developers and provides a PaaS offering for application development. The production systems consist of multi-tier virtualized architecture consisting of web and database servers, storage and content delivery systems, and network and application monitoring tools. A firewall system is also used to restrict information from unauthorized sources and prevent unauthorized network connections.

As part of the cloud computing and data center hosting services, the colocation data centers are responsible for providing the physical safeguarding of the IT infrastructure to help ensure that unauthorized access to the IT infrastructure does not occur, as well as providing environmental safeguards (e.g., uninterrupted power supply, temperature control, fire suppression, etc.) against certain environmental threats.

People

The following personnel are involved in the operation and maintenance of DigitalOcean's services:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Security and Privacy – responsible for creating policies, standards, and procedures that relate to and enforce the risk, governance, privacy, and compliance posture of the organization.
- CloudOps / Product – responsible for designing, building, and maintaining products while adhering to data protection, privacy, and security standards.
- Data Center Operations – responsible for access provisioning and deprovisioning requests made to colocation data center providers.
- IT – responsible for management of employee endpoints and employee account lifecycle management.
- People Operations – responsible for talent acquisition, talent strategy, and total rewards.
- Legal – responsible for general counsel operations and external facing policies and terms.
- Customer Success and Support – responsible for troubleshooting and resolving customer software usage issues.

Procedures

HR and Training

DigitalOcean's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, disciplinary activities, and termination. Defined job descriptions are documented and utilized to outline the required skills needed to successfully fill a position, as well as the job's associated responsibilities, and established pre-hire screening procedures are performed as a component of the hiring process for new personnel based on DigitalOcean's hiring policies and procedures. Personnel are provided with information

security policies, the acceptable use policy, and an employee handbook so that the responsibility and accountability for upholding business values and organizational policies / procedures is clear.

DigitalOcean managers perform semi-annual performance reviews and regular one-on-one meetings with each of their direct reports to evaluate the employees' competency and skills needed to fulfill their job responsibilities. Additionally, during these evaluations, management determines whether the employee adheres to expected conduct and upholds DigitalOcean values. To ensure employees are aware of their responsibility for complying with corporate and business unit security policies, workforce members are required to complete a security awareness training upon hire and annually thereafter. Furthermore, optional training courses are also made available for employees to maintain and further develop their proficiency in their given areas of expertise.

Access, Authentication, and Authorization

Access to DigitalOcean system information, including confidential information, is protected by authentication and authorization mechanisms, which are defined in documented policies and procedures to help guide personnel in logical security requirements. The documented policies and procedures provide guidance to personnel in information security practices such as password requirements, the acceptable use of company resources, access provisioning, and access removal.

Authorized user account and password, with minimum password settings, multi-factor authentication ("MFA"), single sign-on ("SSO"), and / or secure shell protocol ("SSH") public key authentication are enforced by the in-scope systems. Users are required to authenticate to the VPN system via SSO and MFA before being granted access to the production environment. In addition to a unique user account, password, and MFA, users are required to authenticate to the operating system and databases using SSH public key authentication. To authenticate to the DigitalOcean Cloud Infrastructure Platform, users are required to authenticate with a unique user account, password, and have the ability to enable MFA. Users also have the option to allow SSO to gain access to the DigitalOcean Cloud Infrastructure Platform. Additionally, administrative access privileges to the aforementioned in-scope systems are restricted to authorized personnel.

Access Requests and Access Revocation

When an employee or contractor (collectively referred to as "workforce members") is hired, a member of the people operations team initiates a ticket within the HR Information System ("HRIS") for the workforce member, which documents the workforce member's name and job function. The ticket is assigned to the workforce member's hiring manager, who is responsible for creating an access request ticket within the IT HelpDesk ticketing system. Management approval is required before access is granted to the workforce member. Once management approval is obtained, IT personnel provision the requested access for the user.

When a workforce member is terminated, termination tasks are created and tracked in the HRIS. For voluntary or planned terminations, the HRIS, via an API integration, triggers automated processes (offboarding automation) on the day of departure to remove the user's access rights, including privileged access rights, to the in-scope SSO identity provider, VPN, operating systems, databases, and firewalls as a component of the termination process. For unplanned terminations, HR personnel notify IT personnel who will trigger the offboarding automation manually.

System Security and Monitoring

Logging and monitoring systems are in place to analyze, identify, and report possible or actual security vulnerabilities or malicious activity on production hosts to the security team. The logging and monitoring systems are configured to alert CloudOps or security team personnel of issues that meet and / or exceed predefined thresholds, at which point the identified findings are investigated and corrective actions are taken, as necessary. Furthermore, a firewall system is configured to filter unauthorized inbound network traffic from the Internet and deny network connections that are not explicitly authorized by a rule.

Documented vulnerability management policies and procedures are in place at DigitalOcean to guide users in discovering vulnerabilities in the entity's assets and correcting them to help keep DigitalOcean's services, software, infrastructure, operating systems, and applications from being exploited. Vulnerability scans are performed on production systems on an at least weekly basis using the vulnerability scanning tool. Detected security vulnerabilities are triaged by the security team and monitored through resolution using the ticketing system. Furthermore, an independent security professional performs a penetration test on an annual basis to identify

potential security vulnerabilities. High-risk penetration findings are communicated to the applicable teams and triaged to determine remediation plans using the ticketing system.

In addition to vulnerability assessments and penetration testing, a bug bounty program is also used to identify and report vulnerabilities and threats. The security team reviews identified vulnerabilities, which are triaged and monitored through resolution using the ticketing system.

Encryption and Anti-malware

Web communication sessions are encrypted using the TLS encryption protocol. Additionally, encrypted VPNs are used for remote access to help ensure the security and integrity of the data passing over the public network. Employee workstations are configured with full disk encryption upon enrollment to prevent unauthorized access of information. An anti-malware software is installed on employee workstations and configured to scan registered endpoints in real time.

Incident Response

Documented incident response policies and procedures are in place, managed by the security team, and made available to internal workforce members via the internal site detailing how an incident is handled through identifying, containing, remediating, and documenting security incidents. A ticketing system is utilized by the security team to track and manage security incidents from response through to resolution.

DigitalOcean classifies security incidents into the following five security incident types:

- Confidentiality
- Integrity
- Availability
- Safety
- Property

Reported security incidents are first triaged by the security team to confirm the existence of a security incident or assess if the incident is a false positive. If the security team determines that the incident requires further investigation, then a ticket is created with the security incident type, date, and description, and the incident is assigned an incident commander. The incident commander is then responsible for delegating incident response roles to the necessary individuals. During the incident evaluation process, the incident commander works with the security team and those assigned to specific incident response roles to document the details of the identification, containment, recovery, and communication of the security incident within the ticketing system.

Change Management

DigitalOcean has implemented policies and procedures to guide personnel in the request, documentation, and approval of DigitalOcean products and services to be added and subsequently managed within the software development platform. Prior to a new service and / or product being added to DigitalOcean's service catalog, it must first undergo the operational acceptance review ("OAR") process, which is in place to help ensure the following:

- Operational aspects of products and services are configured in a consistent and supportable way following DigitalOcean's existing platforms, standards, and best practices.
- The CloudOps and the product teams have clear visibility and understanding of the upcoming products and services entering the production environment for them to be adequately prepared.
- Ownership and escalation paths for products and services are clear and well defined.
- Operational points of contact are allocated from both the CloudOps and the product teams.
- Providing an opportunity for the product team to hand-off repeatable maintenance and operational upkeep tasks to CloudOps.

The OAR process is mandatory for new SEV-1 products and services that will be in production and/or are customer facing. The severity rating is determined by product or service team owners and CloudOps personnel as a component of the OAR process. Additionally, although not mandatory, the OAR process may be utilized for other new products and services that are not assigned a severity level of one. The OAR process is initiated by the product team owners who work with CloudOps personnel to determine the required tasks needed to create the new product

or service. Additionally, a CloudOps point of contact is assigned to the prospective service and becomes responsible for helping to ensure each subtask associated with the added product or service is completed before it is made available. Once the process is initiated, a ticketing system is utilized to document, track, and manage the agreed upon subtasks associated with the added product or service. Additionally, the OAR ticket is used to define base information associated with the added product or service including, but not limited to, the communication method used to initiate the process, the product or service name, and the CloudOps point of contact.

DigitalOcean utilizes an automated deployment tool to support a continuous integration / continuous deployment ("CI / CD") model for managing infrastructure as code. Additionally, a software development platform is utilized to centrally document, manage, and monitor change requests through implementation. A production pipeline is configured within the automated deployment tool for each added product or service as a component of the OAR process. Once a pipeline build is created within the automated deployment tool, changes made within the software development platform undergo the configured steps included in the build. These configured build steps include a requirement for automated testing of changes made to the production environment for products and services with a defined severity rating of one or two.

At the time of creation, pipeline builds are configured to alert release engineering personnel upon alterations being made to the pipeline build configurations, which include the automated testing requirement for products and services with a defined severity level of one or two. The ability to make such changes to pipeline builds for products and services with a defined severity level of one or two is restricted to authorized personnel. Additionally, pipeline builds are configured to require validation testing for changes to existing pipeline builds within the automated deployment tool to help ensure that alterations will not negatively impact the build and deployment of the infrastructure changes.

Business Continuity and Disaster Recovery

The Architecture team runs a Technical Risk Program that considers the identification, assessment, and prioritization of technical risks which can impact the availability of customer-facing services and/or achievement of the company's business objectives. Risks are formally documented, analyzed, and presented to the audit committee on at least a semi-annual basis.

The Architecture team monitors and triages technical risks impacting customer-facing services and/or achievement of the company's business objectives on a biweekly basis. Identified technical risks are triaged and monitored through resolution via the Technical Risk Program.

The DigitalOcean engineering team dedicated to platform availability and resiliency meets on a weekly basis to review incident trends, post-incident reviews ("PIR"), and action items affiliated with PIRs. These action items consider the time to detect, severity, root cause, impact to availability, and customer impact of incidents. The engineering team also performs a tabletop exercise annually to review the recovery procedures to ensure they are functioning to standard.

Media Disposal / Destruction

Asset removal and disposal policies are in place to guide personnel in the disposal of assets to help ensure data and software is unrecoverable prior to decommissioning physical assets. Physical assets are securely destroyed or erased prior to decommissioning or reprovisioning the assets. The process of decommissioning physical assets is to be completed in accordance with the documented asset removal and disposal policies and decommissioned physical assets are logged within the data center asset management software. Third parties are contracted to destroy physical hardware maintained at colocation data centers prior to asset disposal. Contracted third parties provide a certificate of destruction upon completion of destruction services for physical production assets.

Vendor Management

Security management considers the identification and assessment of risks and mitigation activities associated with vendors and business partners during the risk assessment and mitigation activities. Furthermore, security personnel perform due diligence on vendors that could potentially store or access customer data by reviewing the vendor's third-party compliance reports or requiring a completed security questionnaire as a component of the onboarding process. DigitalOcean's security commitments and obligations, including those made the responsibility of DigitalOcean's vendors and business partners are further documented and communicated through the terms of service made available via the company's website. Ongoing relationships with vendors are evaluated during the contract renewal process, just as during onboarding.

Access to Colocation Facilities

New and modified workforce member access to colocation data centers is required to be documented within the ticketing system upon communication of the request to the respective colocation data center. Physical access termination requests for workforce members are documented in the ticketing system as a component of the termination process.

Data

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

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Droplet Metadata	Droplet metadata can be accessed using the client URL command line tool with a special static IP address.	Restricted
Droplet User Data	User data is provided to a droplet when it's created and cannot be modified thereafter. The data can be accessed using the client URL command line tool.	
Stored Files	Files are stored in buckets, which are used as part of the spaces object storage service. The data stored in the buckets is accessible by authorized user personnel controlled via restricted access keys.	
DOKS Cluster Metrics	DOKS includes metrics to provide insight into the health of a user's Kubernetes clusters and deployments. Metric data is made available via the user's DigitalOcean overview page that is accessible by authorized user personnel.	
App Platform Logs	Logs are captures of the activity related to the user's application. Logs are available to authorized user personnel via the control plane or from the command line.	
Infrastructure, Service, and Secondary Program Logs	Available to users via database storage for which access is restricted to authorized user personnel.	

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 data center hosting services provided by colocation data centers 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 colocation data centers, alone or in combination with controls at DigitalOcean, and the types of controls expected to be implemented at colocation data centers to achieve DigitalOcean'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	Colocation data centers are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.	CC6.4, CC6.5
CSOC.02	Colocation data centers are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.	A1.2

CONTROL ENVIRONMENT

The control environment at DigitalOcean 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 DigitalOcean's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of DigitalOcean's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, and by example. In certain circumstances control activities implemented by the service organization apply to employees alone, while others apply to employees and contractors, which are collectively referred to as "workforce members." Specific control activities that the service organization has implemented in this area are described below:

- Workforce members are required to sign acknowledgement forms upon hire and annually thereafter to acknowledge that they have read and understood the acceptable use policy.
- Background checks are performed for workforce members as a component of the hiring process.
- Policies are documented and maintained (acceptable use and security training) that address expected behaviors and responsibilities. The policies are communicated to employees via the company's internal site.
- Employee evaluations include a component of achieving company values (which includes acting with integrity and in an ethical manner).
- A whistleblower policy is communicated to employees for anonymous reporting of incidents, concerns, and other complaints via a whistleblower hotline.

- Security management monitors potentially fraudulent related risks using the data analytics platform and provides updates to the CEO on a monthly basis regarding revenues generated from the potentially fraudulent use of DigitalOcean services.

Board of Directors and Audit Committee Oversight

DigitalOcean is a publicly traded company and therefore must adhere to certain organizational and oversight requirements. A board of directors is charged with oversight of senior management and with the responsibility to provide direction to the organization. The audit committee is a subcommittee of the board of directors and is in charge of overseeing the systems of internal control at DigitalOcean. Board and audit committee are, by majority, independent of management.

The executive team at DigitalOcean meets with the board of directors and the audit committee on a semi-annual basis to provide updates to financial performance, operational performance, updated risks, and associated metrics. Relevant findings from internal audits are also presented. An analysis of these performance metrics are presented as well as the overall impact on the business and organizational goals.

Organizational Structure and Assignment of Authority and Responsibility

DigitalOcean's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. DigitalOcean's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and proper lines of reporting. DigitalOcean has developed an organizational structure suited to its needs and based, in part, on its size and the nature of its activities.

DigitalOcean's assignment of authority and responsibility includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for performing duties. In addition, it includes policies and communications directed at helping to ensure personnel understand the entity's objectives, understand how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

To further set the tone for authority and responsibility, management has assigned the responsibility of the maintenance and enforcement of information security policies and procedures to the DigitalOcean security and leadership teams. Organizational charts are in place to communicate key areas of authority, responsibility, and proper lines of reporting to personnel. The organizational charts are made available to employees through the company's internal site and help management define authority and responsibility. Additionally, to communicate the expected behavior and skills needed to facilitate the accomplishment of business objectives, DigitalOcean has documented position descriptions to define the skills, responsibilities, knowledge levels required for particular jobs, and the direct lines of reporting for employees.

Commitment to Competence

DigitalOcean's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. DigitalOcean's commitment to competence includes management's consideration of the competence levels for particular jobs during candidate screening and how those levels translate into requisite skills and knowledge. As part of the interview and onboarding process, managers evaluate competencies based on the required skills defined in the written position descriptions. More specifically, members of the security team are vetted for their skills and competencies as it relates to the security team's job function.

A security awareness training program is in place to guide employees in understanding their obligations and responsibilities to comply with the corporate and business unit security policies. To develop and retain competent personnel, ongoing training and learning programs, which includes an education reimbursement benefit program, are made available to DigitalOcean employees. Through these programs and through the dedicated budget for the ongoing skill development of its employees, DigitalOcean is committed to maintaining a high level of performance amongst their team members.

Accountability

DigitalOcean's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, as well as management's attitudes toward holding themselves and DigitalOcean personnel accountable for their duties. Specific control activities that DigitalOcean has implemented in this area are described below:

- Reporting lines are communicated to personnel so that awareness of responsibility and ownership of various functions and personnel is clear.
- Management conducts a performance review of employees on a semi-annual basis to evaluate performance of employees against expected levels of performance.
- Workforce members are required to complete security awareness training upon hire and annually thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.

RISK ASSESSMENT

Objective Setting

The risk assessment is a dynamic process that includes identification and analysis of risks that pose a threat to the organization's ability to perform its in-scope services. The risk assessment process starts with determining the organization's objectives. To do so, DigitalOcean's security management team meets with the audit committee and board of directors on an annual basis to review financial performance metrics, operational performance metrics, and help ensure its business objectives remain appropriate. During the aforementioned meeting, security management discusses how the organization aligns the performance measures and incentives with company business objectives.

Risk Identification and Analysis

DigitalOcean has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Management identifies risks to the achievement of its objectives and analyzes those risks as a basis for determining how risks should be managed. Documented risk management policies and procedures are in place to guide personnel in identifying risks to the achievement of the organization's objectives, assessing changes to the system, and developing risk mitigation strategies as a part of the risk assessment process.

Security management performs a risk assessment annually that includes the identification and analysis of the entity's business and security risks and vulnerabilities. DigitalOcean uses a risk rating system based on likelihood and impact to determine each risk's severity level. The risk evaluation process also accounts for changes in risks from the prior assessments / evaluations, considers changes to the system, and assesses changes that could significantly impact the system of internal control. Furthermore, the security team maintains a business risk matrix that tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities.

Risk Factors

Management considers risks that can arise from both external and internal factors including 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
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Security management considers the potential for fraud when assessing the risks to the company's objectives. Security management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. As such, DigitalOcean's security considers the potential for fraud as it relates to IT as part of the annual risk assessment process.

Security management further monitors fraud risks related to the misuse of DigitalOcean services using a data analytics platform. Results identified in the data analytics platform are monitored and an update is provided to the CEO on a quarterly basis.

Risk Mitigation

Documented policies and procedures are in place to guide DigitalOcean personnel in identifying, selecting, and developing mitigating activities for risks identified as part of the annual risk assessment process. Security management selects and develops control activities to mitigate the risks identified during the annual risk assessment process. Security management personnel are responsible for selecting and developing control activities to mitigate risks identified during the risk assessment process. The control activities are documented within the mitigation plans for controls above the tolerable threshold and include control activities over technology. Risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives. The completed risk assessment and business risk matrix, along with mitigation strategies, are documented for the audit committee's review.

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. 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 and availability 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 DigitalOcean'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 and availability categories are applicable to the Cloud Infrastructure Platform system.

Information and Communication Systems

Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information, which make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. DigitalOcean generates and uses relevant, quality information in a variety of ways including the use of log monitoring systems, vulnerability assessments, a bug bounty program, and through the communication of the results of penetration tests to identify and remediate potential security vulnerabilities.

Effective communication also must occur in a broader sense, flowing down, across and up the organization. Personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, and how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Internal Communications

DigitalOcean has implemented various methods of communication to help provide assurance that significant events are communicated. These methods include maintaining documented information security policies that relate to activities such as information security risk management, acceptable use of hardware, data communications, system monitoring, data security, and access management. Additionally, a whistleblower hotline, which is communicated to employees via the company's learning management system ("LMS") is accessible by internal workforce members to report incidents, concerns, and complaints.

External Communications

DigitalOcean has also implemented methods of communication to help provide assurance that customers understand the roles and responsibilities around the communication of significant events. These methods include providing external users with a customer support channel made available via the company's website to report security incidents, concerns, and complaints that relate to potential system abuse. DigitalOcean communicates its security commitments and associated system requirements, including security, contractual, and regulatory requirements to external users on the company's website via the company's terms of service that customers are required to acknowledge at the time of account creation. External parties are also notified of changes to

DigitalOcean's terms of service and privacy policy via e-mail and / or the company's website. Landing pages are maintained on the company's website and used to communicate changes and maintenance activities affecting system security and availability via release notes and other communications. Additionally, relevant information regarding internal controls and corporate governance is available on the 'Investor Relations' page on the DigitalOcean website.

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.

Ongoing Monitoring

By monitoring the risks and the effectiveness of control measures on a regular basis, DigitalOcean can react dynamically to changing conditions. DigitalOcean utilizes both manual and automated monitoring tools to monitor control activities, including the following:

- Logging and monitoring systems are utilized to collect and analyze security vulnerabilities, system performance, and resource utilization data from in-scope systems. The logging and monitoring systems are configured to send push notifications to CloudOps personnel upon predefined thresholds being met and/or exceeded regarding system performance. The systems are configured to send push notifications to security team personnel upon predefined thresholds being met and/or exceeded regarding security vulnerabilities and resource utilization. Alerts are then investigated, and corrective actions are taken, as necessary.
- Security management considers the impact of changes to applicable laws or regulations during the annual risk assessment process.
- Executive management team meetings provide important feedback to the audit committee on whether controls are effective.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

DigitalOcean's security team reviews third-party compliance reports or completed security questionnaires as a component of the onboarding process for third-party vendors and/or business partners requiring access to customer data, to help ensure that the third-party providers are in compliance with the organization's security requirements.

Evaluations also take the form of periodic assessments such as vulnerability assessments, penetration tests, and DigitalOcean's bug bounty program. Identified areas of deficiency or concern are reviewed by management and tracked formally to help ensure that potential breakdowns in controls or security are resolved.

Subservice Organization Monitoring

DigitalOcean utilizes the services of colocation data center service providers to host its computing hardware and servers. Performance is regularly monitored as part of day-to-day business operations. More formally, DigitalOcean makes a listing of its data centers publicly available via the company's website, along with the most recently completed third-party compliance certifications obtained for each respective colocation facility which include the respective location's physical and environmental controls. These colocation data center providers are further monitored according to vendor management procedures.

Evaluating and Communicating Deficiencies

Management has developed protocols to help ensure findings of internal control deficiencies are reported to the individuals responsible for the function or activity involved and are in a position to take corrective action. This process enables responsible individuals to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected.

Deficiencies in the internal control system may surface from multiple sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. To facilitate the evaluation and communication of internal control deficiencies, DigitalOcean's security team maintains security incident response procedures for reporting security incidents, concerns, and other complaints. Furthermore, security incident response channels are utilized by internal users to report security incidents. A customer support channel is utilized and made available on the company's website to provide external parties with a channel to report security incidents, concerns, or abuse in relation to misuse of DigitalOcean's services. Security management also presents documented internal control performance metrics to the audit committee on an annual basis.

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 User Entity Controls

DigitalOcean'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.

Complementary User Entity Control Responsibilities

As mentioned above, DigitalOcean'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.

However, in order for user entities to benefit from the Cloud Infrastructure Platform system and its controls, the following responsibilities should be considered by user entities:

Ref.	Control Responsibilities to be Considered by User Entities
1	User entities are responsible for ensuring the supervision, management, and control of the use of DigitalOcean's services by their personnel.
2	User entities are responsible for understanding and complying with their contractual obligations to DigitalOcean.
3	User entities are responsible for immediately notifying DigitalOcean of any actual or suspected security breaches, including compromised user accounts.
4	User entities are responsible for the security and privacy of data while using DigitalOcean products.

Ref.	Control Responsibilities to be Considered by User Entities
5	User entities are responsible for establishing and maintaining strong passwords and secure single sign-on and/or multi-factor authentication credentials to the DigitalOcean user interface.
6	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize DigitalOcean services.
7	User entities are responsible for developing their own data backup procedures that address the inability to access or utilize DigitalOcean services.
8	User entities are responsible for ensuring the supervision, management, and control of the use of DigitalOcean's services by their personnel.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Cloud Infrastructure Platform system provided by DigitalOcean. The scope of the testing was restricted to the Cloud Infrastructure Platform system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period January 1, 2025, to December 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	(Control 1) Senior management's commitment to implementing, maintaining, and continually improving the security risk posture includes the implementation of an acceptable use policy and employee security training.	Inspected the acceptable use policy and the security rule roles policy to determine that senior management's commitment to implementing, maintaining, and continually improving the security risk posture included the implementation of an acceptable use policy and employee security training.	No exceptions noted.
CC1.1.2	(Control 69) Workforce members are required to review and acknowledge the acceptable use policy upon hire and annually thereafter.	Inspected the acceptable use policy acknowledgement for a sample of workforce members hired during the period to determine that workforce members were required to review and acknowledge the acceptable use policy upon hire for each workforce member sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the acceptable use policy acknowledgement for a sample of current workforce members to determine that workforce members were required to review and acknowledge the acceptable use policy during the period for each workforce member sampled.	No exceptions noted.
CC1.1.3	(Control 2) Employees receive performance evaluations semi-annually to evaluate the employee's adherence to company values, competency, and skills to fulfill job responsibilities.	Inspected the most recent completed performance evaluation for a sample of current employees to determine that employees received performance evaluations to evaluate the employee's adherence to company values, competency, and skills to fulfill job responsibilities during the period for each employee sampled.	No exceptions noted.
CC1.1.4	(Control 26) Background screening is performed for workforce members as a component of the hiring process.	Inspected the completed background check for a sample of workforce members hired during the period to determine that background screening was performed as a component of the hiring process for each workforce member sampled.	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	(Control 32) Board of directors and audit committee charters are documented detailing the responsibility for the oversight of management and internal control.	Inspected the board of directors and audit committee charters to determine that board of directors and audit committee charters were documented detailing the responsibility for the oversight of management and internal control.	No exceptions noted.
CC1.2.2	(Control 44) The board of directors is comprised of members who are, by majority, independent of management and objective in evaluation and decision making.	Inspected the board of directors charter and member listing to determine that the board of directors was comprised of members who were, by majority, independent of management and objective in evaluation and decision making.	No exceptions noted.
CC1.2.3	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	(Control 4) DigitalOcean has an organizational chart that defines reporting lines and is communicated to employees via the company's internal site.	Inspected the organizational chart on the corporate intranet to determine that DigitalOcean had an organizational chart that defined reporting lines and was communicated to employees via the company's internal site.	No exceptions noted.
CC1.3.2	(Control 5) Management has defined job descriptions to document and communicate the roles and responsibilities of employment positions for new hires.	Inspected the documented job description for a sample of employment positions to determine that management had defined job descriptions for new hires to document and communicate the roles and responsibilities for each position sampled.	No exceptions noted.
CC1.3.3	(Control 29) Management personnel have assigned the responsibility of the maintenance and enforcement of the entity's security policies and procedures to the DigitalOcean security and leadership teams.	Inspected the security rule roles policy to determine that management personnel had assigned the responsibility of the maintenance and enforcement of the entity's security policies and procedures to DigitalOcean security and leadership teams.	No exceptions noted.
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	(Control 29) Management personnel have assigned the responsibility of the maintenance and enforcement of the entity's security policies and procedures to the DigitalOcean security and leadership teams.	Inspected the security rule roles policy to determine that management personnel had assigned the responsibility of the maintenance and enforcement of the entity's security policies and procedures to DigitalOcean security and leadership teams.	No exceptions noted.
CC1.4.2	(Control 7) Management personnel conduct job interviews for security team applicants to verify the technical competency of prospective security team members.	Inspected the employment and technical screening documentation for a sample of security team employees hired during the period to determine that management personnel conducted job interviews for security team applicants to verify the technical competency of prospective security team members for each workforce member sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	(Control 2) Employees receive performance evaluations semi-annually to evaluate the employee's adherence to company values, competency, and skills to fulfill job responsibilities.	Inspected the most recent completed performance evaluation for a sample of current employees to determine that employees received performance evaluations to evaluate the employee's adherence to company values, competency, and skills to fulfill job responsibilities during the period for each employee sampled.	No exceptions noted.
CC1.4.4	(Control 70) Workforce members are required to complete a security awareness training upon hire and annually thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training program and the security awareness training completion documentation for a sample of workforce members hired during the period to determine that workforce members were required to complete a security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies for each workforce member sampled.	No exceptions noted.
		Inspected the security awareness training program and the security awareness training completion documentation for a sample of current workforce members to determine that workforce members were required to complete a security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period for each workforce member sampled.	No exceptions noted.
CC1.4.5	(Control 59) Ongoing learning opportunities are offered to employees via an education reimbursement benefit program and an online training platform to help ensure that employees maintain and advance their skill levels.	Inspected the learning management system dashboard, the education reimbursement policy, and the education reimbursement portal to determine that ongoing learning opportunities were offered to employees via an education reimbursement benefit program and an online training platform to help ensure that employees maintained and advanced their skill levels.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	(Control 5) Management has defined job descriptions to document and communicate the roles and responsibilities of employment positions for new hires.	Inspected the documented job description for a sample of employment positions to determine that management had defined job descriptions for new hires to document and communicate the roles and responsibilities for each position sampled.	No exceptions noted.
CC1.5.2	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business during the period.	No exceptions noted.
CC1.5.3	(Control 2) Employees receive performance evaluations semi-annually to evaluate the employee's adherence to company values, competency, and skills to fulfill job responsibilities.	Inspected the most recent completed performance evaluation for a sample of current employees to determine that employees received performance evaluations to evaluate the employee's adherence to company values, competency, and skills to fulfill job responsibilities during the period for each employee sampled.	No exceptions noted.
CC1.5.4	(Control 70) Workforce members are required to complete a security awareness training upon hire and annually thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training program and the security awareness training completion documentation for a sample of workforce members hired during the period to determine that workforce members were required to complete a security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies for each workforce member sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security awareness training program and the security awareness training completion documentation for a sample of current workforce members to determine that workforce members were required to complete a security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period for each workforce member sampled.	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	(Control 6) Documented policies and procedures are in place to guide personnel in information security activities that include, but are not limited to, the following: • Access management • Risk management • Incident response management • System monitoring • Change management • Data security	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in information security activities that included the following: • Access management • Risk management • Incident response management • System monitoring • Change management • Data security	No exceptions noted.
CC2.1.2	(Control 31) Logging and monitoring systems are configured to collect data from in-scope production hosts to analyze potential security vulnerabilities based on criticality and to alert the security team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope production hosts to analyze security vulnerabilities based on criticality and to alert security team personnel when predefined thresholds were met and/or exceeded.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.3	(Control 63) Logging and monitoring systems are configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC2.1.4	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.
CC2.1.5	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC2.1.6	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC2.1.7	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business 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	(Control 6) Documented policies and procedures are in place to guide personnel in information security activities that include, but are not limited to, the following: • Access management • Risk management • Incident response management • System monitoring • Change management • Data security	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in information security activities that included the following: • Access management • Risk management • Incident response management • System monitoring • Change management • Data security	No exceptions noted.
CC2.2.2	(Control 62) Security incident response channels are made available to employees to report potential and actual security incidents to security personnel.	Inspected the security incident response submission channel to determine that security incident response channels were made available to employees to report potential and actual security incidents to security personnel.	No exceptions noted.
CC2.2.3	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business during the period.	No exceptions noted.
CC2.2.4	(Control 60) A whistleblower policy is communicated to employees via the company's LMS and includes instructions for anonymous reporting of incidents, concerns, and other complaints via a whistleblower hotline.	Inspected the whistleblower policy and the policy training curriculum to determine that a whistleblower policy was communicated to employees via the company's LMS and included instructions for anonymous reporting of incidents, concerns, and other complaints via a whistleblower hotline.	No exceptions noted.
CC2.2.5	(Control 69) Workforce members are required to review and acknowledge the acceptable use policy upon hire and annually thereafter.	Inspected the acceptable use policy acknowledgement for a sample of workforce members hired during the period to determine that workforce members were required to review and acknowledge the acceptable use policy upon hire for each workforce member sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the acceptable use policy acknowledgement for a sample of current workforce members to determine that workforce members were required to review and acknowledge the acceptable use policy during the period for each workforce member sampled.	No exceptions noted.
CC2.2.6	(Control 70) Workforce members are required to complete a security awareness training upon hire and annually thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training program and the security awareness training completion documentation for a sample of workforce members hired during the period to determine that workforce members were required to complete a security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies for each workforce member sampled.	No exceptions noted.
		Inspected the security awareness training program and the security awareness training completion documentation for a sample of current workforce members to determine that workforce members were required to complete a security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period for each workforce member sampled.	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	(Control 12) Customers are required to acknowledge that they have read and agree to the company's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements that are documented on the company's website within the terms of service.	Inspected the DigitalOcean user registration page and the legal and security documents available on the company's website to determine that customers were required to acknowledge that they had read and agreed to the company's security commitments and the associated system requirements, including the security, contractual, and regulatory requirements that were documented on the company's website within the terms of service.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.2	(Control 13) The Terms of Service and Privacy policy is made available to customers via the company website.	Inquired of the manager of governance, risk, and compliance regarding the terms of service and privacy policy to determine the Terms of Service and Privacy policy was made available to customers via the company website.	No exceptions noted.
		Inspected the terms of service policy to determine that the Terms of Service and Privacy policy was made available to customers via the company website.	No exceptions noted.
CC2.3.3	(Control 14) Landing pages are maintained on the company's website to communicate the following: • Release notes for changes to the DigitalOcean cloud platform • Service interruptions, performance degradation, scheduled maintenance, and other issues affecting customers	Inspected the release notes and system status pages on the company's website to determine that landing pages were maintained on the company's website to communicate the following: • Release notes for changes to the DigitalOcean cloud platform • Service interruptions, performance degradation, scheduled maintenance, and other issues affecting customers	No exceptions noted.
CC2.3.4	(Control 15) A customer support channel for reporting abuse on sites hosted by DigitalOcean is made available to external parties on the company's website.	Inspected the customer support portal on the company's website to determine that a customer support channel for reporting abuse on sites hosted by DigitalOcean was made available to external parties on the company's website.	No exceptions noted.
CC2.3.5	(Control 71) Relevant information regarding internal controls and corporate governance is available on the "Investor Relations" page of the DigitalOcean website.	Inspected the DigitalOcean website to determine that relevant information regarding internal controls and corporate governance was available on the "Investor Relations" page of the DigitalOcean website.	No exceptions noted.
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	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	(Control 16) Security management performs a risk assessment on at least an annual basis that considers the identification and assessment of risks relating to the company's operations, safeguarding of informational assets, and changes in technology or client relationships.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the identification and assessment of risks relating to the company's operations, safeguarding of informational assets, and changes in technology or client relationships during the period.	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	(Control 17) Security management performs a risk assessment on at least an annual basis to identify, evaluate, and track business and security risks, vulnerabilities, laws, and regulations. Identified risks are formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment to identify, evaluate, and track business and security risks, vulnerabilities, laws, and regulations and that identified risks were formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies during the period.	No exceptions noted.
CC3.2.2	(Control 18) The security team maintains a business risk matrix that tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities that is reviewed by the audit committee on at least an annual basis.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that the security team maintained a business risk matrix that tracked identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities that was reviewed by the audit committee during the period.	No exceptions noted.
CC3.2.3	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.
CC3.2.4	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC3.2.5	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	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	(Control 55) Security management performs a risk assessment on at least an annual basis that considers the potential for fraud. Identified risks are formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the potential for fraud and that identified risks were formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies during the period.	No exceptions noted.
CC3.3.2	(Control 46) Security management monitors fraud-related risks using the data analytics platform and updates the CEO on at least a quarterly basis about revenue generated from potentially fraudulent use of DigitalOcean services.	Inspected the data analytics platform dashboard and the security meeting invite, listing of attendees, and agenda overview for a sample of quarters during the period to determine that security management monitored fraud related risks using the data analytics platform and updated the CEO about revenue generated from potentially fraudulent use of DigitalOcean services for each quarter sampled.	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	(Control 73) Security management performs a risk assessment on at least an annual basis that considers the impact of changes to the system. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, formally documented, and reviewed by the audit committee.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the impact of changes to the system and that identified risks were rated using a risk evaluation process that accounted for changes in risk from the prior year, formally documented, and reviewed by the audit committee during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.2	(Control 18) The security team maintains a business risk matrix that tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities that is reviewed by the audit committee on at least an annual basis.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that the security team maintained a business risk matrix that tracked identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities that was reviewed by the audit committee during the period.	No exceptions noted.
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	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.
CC4.1.2	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC4.1.3	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC4.1.4	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business during the period.	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	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.
CC4.2.2	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.3	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC4.2.4	(Control 45) DigitalOcean's security team meets with the audit committee and board of directors on at least an annual basis to review financial performance metrics, operational performance metrics, and risks to the business.	Inspected the meeting invite, listing of attendees, and agenda for the most recent audit committee meeting to determine that DigitalOcean's security team met with the audit committee and board of directors to review financial performance metrics, operational performance metrics, and risks to the business during the period.	No exceptions noted.
CC4.2.5	(Control 62) Security incident response channels are made available to employees to report potential and actual security incidents to security personnel.	Inspected the security incident response submission channel to determine that security incident response channels were made available to employees to report potential and actual security incidents to security personnel.	No exceptions noted.
CC4.2.6	(Control 11) Documented security incident response procedures are in place, managed by the security incident response team, and used to guide employees in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the security incident response playbook on the corporate intranet to determine that documented security incident response procedures were in place, managed by the security incident response team, and used to guide employees 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
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	(Control 8) Security management performs a risk assessment on at least an annual basis that considers the identification and assessment of risks relating to the company's business objectives. Identified risks are formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the identification and assessment of risks related to the company's business objectives and that identified risks were formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies during the period.	No exceptions noted.
CC5.1.2	(Control 18) The security team maintains a business risk matrix that tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities that is reviewed by the audit committee on at least an annual basis.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that the security team maintained a business risk matrix that tracked identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities that was reviewed by the audit committee 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	(Control 22) Documented policies and procedures are in place to guide personnel in information security activities related to technology that include, but are not limited to, the following: • Acceptable use • Mobile device management • Data security • Access management • Change management	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in information security activities related to technology that included the following: • Acceptable use • Mobile device management • Data security • Access management • Change management	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.2	(Control 56) Security management performs a risk assessment on at least an annual basis that considers the identification and assessment of technology risks that can impact the achievement of the company's business objectives. Identified risks are formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the identification and assessment of technology risks that could impact the achievement of company's business objectives and that identified risks were formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies 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	(Control 6) Documented policies and procedures are in place to guide personnel in information security activities that include, but are not limited to, the following: • Access management • Risk management • Incident response management • System monitoring • Change management • Data security	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in information security activities that included the following: • Access management • Risk management • Incident response management • System monitoring • Change management • Data security	No exceptions noted.
CC5.3.2	(Control 69) Workforce members are required to review and acknowledge the acceptable use policy upon hire and annually thereafter.	Inspected the acceptable use policy acknowledgement for a sample of workforce members hired during the period to determine that workforce members were required to review and acknowledge the acceptable use policy upon hire for each workforce member sampled.	No exceptions noted.
		Inspected the acceptable use policy acknowledgement for a sample of current workforce members to determine that workforce members were required to review and acknowledge the acceptable use policy during the period for each workforce member sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	(Control 70) Workforce members are required to complete a security awareness training upon hire and annually thereafter to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training program and the security awareness training completion documentation for a sample of workforce members hired during the period to determine that workforce members were required to complete a security awareness training upon hire to understand their obligations and responsibilities to comply with the corporate and business unit security policies for each workforce member sampled.	No exceptions noted.
		Inspected the security awareness training program and the security awareness training completion documentation for a sample of current workforce members to determine that workforce members were required to complete a security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies during the period for each workforce member sampled.	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	(Control 21) Documented logical access policies and procedures are in place to guide personnel in information security practices that include, but are not limited to, the following: • Password requirements • Acceptable use • Access provisioning • Access termination	Inspected the logical access policies and procedures to determine that documented policies and procedures were in place to guide personnel in information security practices that included the following: • Password requirements • Acceptable use • Access provisioning • Access termination	No exceptions noted.
CC6.1.2	(Control 25) The in-scope systems are configured to require at least one of the following authentication requirements prior to granting users access to the system: • Authorized user account and password • MFA • SSO • SSH	Inspected the SSO identity provider authentication configurations to determine that the SSO identity provider was configured to require an authorized user account and password and MFA prior to granting users access to the system.	No exceptions noted.
		Inspected the VPN authentication configurations to determine that the VPN was configured to require SSO prior to granting users access to the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the firewall management system authentication configurations to determine that the production firewalls were configured to require SSO prior to granting users access to the system.	No exceptions noted.
		Inspected the authentication configurations for a sample of in-scope production servers to determine that the production servers were configured to require SSH prior to granting users access to the system for each server sampled.	No exceptions noted.
		Inspected the authentication configurations for a sample of in-scope production databases to determine that the production databases were configured to require SSH prior to granting users access to the system for each database sampled.	No exceptions noted.
		Inspected the DigitalOcean end user portal authentication configurations to determine that the DigitalOcean portal was configured to require an authorized user account and password prior to granting users access to the system.	No exceptions noted.
		Inspected the software development platform authentication configurations to determine that the software development platform was configured to require an authorized user account and password and MFA prior to granting users access to the system.	No exceptions noted.
CC6.1.3	(Control 27) Administrative and privileged access to the in-scope systems is restricted to user accounts accessible by authorized personnel.	Inspected the SSO identity provider administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the SSO identity provider was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the VPN administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the VPN was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the firewall management system administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the production firewalls was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the administrator access listings for a sample of in-scope production servers with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the production servers was restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
		Inspected the administrator access listings for a sample of in-scope production databases with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the production databases was restricted to user accounts accessible by authorized personnel for each database sampled.	No exceptions noted.
		Inspected the software development platform administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the software development platform was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	(Control 3) Requests for new and modified workforce member system access are documented in the ticketing system and require the approval from the workforce member's manager or system owner prior to access being granted.	Inspected the access request ticket for a sample of workforce members granted new or modified system access during the period to determine that requests for new and modified workforce member system access were documented in the ticketing system and required the approval from the workforce member's manager or system owner prior to access being granted for each workforce member sampled.	No exceptions noted.
CC6.2.2	(Control 28) IT personnel follow a termination workflow and revoke terminated workforce member access rights to in-scope systems as a component of the termination process.	Inspected the deactivated employee status and the automated deprovisioning configuration for a sample of employees terminated during the period to determine that IT personnel followed a termination workflow as a component of the termination process for each workforce member sampled.	No exceptions noted.
		Inspected the production system user listings for a sample of employees terminated during the period to determine that system access was revoked for workforce members as a component of the termination process for each workforce member sampled.	No exceptions noted.
CC6.2.3	(Control 68) Security personnel complete a review of user accounts with access to the following in-scope systems on an at least annual basis: • SSO platform • VPN • Firewalls • Kubernetes clusters • Databases	Inspected the results of the most recently completed user access review to determine that security personnel completed a review of user accounts with access to the following in-scope systems during the period: • SSO identity provider • VPN • Firewalls • Kubernetes clusters • Databases	No exceptions noted.

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	(Control 3) Requests for new and modified workforce member system access are documented in the ticketing system and require the approval from the workforce member's manager or system owner prior to access being granted.	Inspected the access request ticket for a sample of workforce members granted new or modified system access during the period to determine that requests for new and modified workforce member system access were documented in the ticketing system and required the approval from the workforce member's manager or system owner prior to access being granted for each workforce member sampled.	No exceptions noted.
CC6.3.2	(Control 28) IT personnel follow a termination workflow and revoke terminated workforce member access rights to in-scope systems as a component of the termination process.	Inspected the deactivated employee status and the automated deprovisioning configuration for a sample of employees terminated during the period to determine that IT personnel followed a termination workflow as a component of the termination process for each workforce member sampled.	No exceptions noted.
		Inspected the production system user listings for a sample of employees terminated during the period to determine that system access was revoked for workforce members as a component of the termination process for each workforce member sampled.	No exceptions noted.
CC6.3.3	(Control 68) Security personnel complete a review of user accounts with access to the following in-scope systems on an at least annual basis: • SSO platform • VPN • Firewalls • Kubernetes clusters • Databases	Inspected the results of the most recently completed user access review to determine that security personnel completed a review of user accounts with access to the following in-scope systems during the period: • SSO identity provider • VPN • Firewalls • Kubernetes clusters • Databases	No exceptions noted.
CC6.3.4	(Control 27) Administrative and privileged access to the in-scope systems is restricted to user accounts accessible by authorized personnel.	Inspected the SSO identity provider administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the SSO identity provider was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the VPN administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the VPN was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the firewall management system administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the production firewalls was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the administrator access listings for a sample of in-scope production servers with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the production servers was restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
		Inspected the administrator access listings for a sample of in-scope production databases with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the production databases was restricted to user accounts accessible by authorized personnel for each database sampled.	No exceptions noted.
		Inspected the software development platform administrator access listing with the assistance of the manager of governance, risk, and compliance to determine that administrative and privileged access to the software development platform was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.4.1	(Control 49) Requests for new and modified workforce member physical access to the DigitalOcean colocation data centers are documented in a ticketing system by a member of the data center operations team.	Inspected the data center security access standard and the physical access request ticket for a sample of employees hired during the period requiring physical access to determine that requests for new and modified workforce member physical access to the DigitalOcean colocation data centers were documented in a ticketing system by a member of the data center operations team for each employee sampled.	No exceptions noted.
CC6.4.2	(Control 50) Data center operations workforce personnel document workforce member physical access revocation to the DigitalOcean data centers in a ticketing system as a component of the termination process.	Inquired of the manager of governance, risk, and compliance regarding physical access to determine that data center operations workforce personnel documented workforce member physical access revocation to the DigitalOcean data centers in a ticketing system as a component of the termination process.	No exceptions noted.
		Inspected the colocation data center access removal user listing reports and determined that no access removal tickets occurred during the period; therefore, no testing of operating effectiveness was performed.	
CC6.4.3	(Control 51) The data center operations team reviews the colocation data center access listings at least annually.	Inspected the most recently completed colocation data center access review to determine that the data center operations team reviewed the colocation data center access listings during the period.	No exceptions noted.
CSOC.01	Colocation data centers are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.		
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	(Control 52) Documented physical asset disposal policies and procedures are in place to guide personnel in rendering data stored on physical media within colocation data centers unreadable prior to disposal.	Inspected the information retention and disposal policies and procedures to determine that documented physical asset disposal policies and procedures were in place to guide personnel in rendering data stored on physical media within colocation datacenters unreadable prior to disposal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.5.2	(Control 53) Third parties are contracted to destroy physical hardware maintained at the colocation data centers.	Inspected the signed third-party agreements for a sample of data center colocation facilities and an example certificate of destruction received during the period to determine that third parties were contracted to destroy physical hardware maintained at the colocation data centers for each facility sampled.	No exceptions noted.
CC6.5.3	(Control 54) Third parties provide a certificate of destruction upon destruction of physical production assets maintained in the colocation data centers.	Inspected the certificate of destruction for a sample of physical production assets disposed of during the period to determine that third parties provided a certificate of destruction upon destruction of physical production assets maintained in the colocation data centers for each disposed physical production asset sampled.	No exceptions noted.
CSOC.01	Colocation data centers are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.		
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	(Control 35) Web communication sessions are encrypted using the TLS encryption protocol.	Inspected the enabled TLS encryption configurations to determine that web communication sessions were encrypted using the TLS encryption protocol.	No exceptions noted.
CC6.6.2	(Control 36) Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the enabled VPN encryption configurations to determine that encrypted VPNs were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.
CC6.6.3	(Control 72) A firewall system is configured to filter unauthorized inbound network traffic from the Internet and deny network connections that are not explicitly authorized by a rule.	Inspected the enabled firewall ruleset configurations to determine that a firewall system was configured to filter unauthorized inbound network traffic from the Internet and deny network connections that were not explicitly authorized by a rule.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.4	(Control 31) Logging and monitoring systems are configured to collect data from in-scope production hosts to analyze potential security vulnerabilities based on criticality and to alert the security team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope production hosts to analyze security vulnerabilities based on criticality and to alert security team personnel when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC6.6.5	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.
CC6.6.6	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC6.6.7	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	No exceptions noted.
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	(Control 35) Web communication sessions are encrypted using the TLS encryption protocol.	Inspected the enabled TLS encryption configurations to determine that web communication sessions were encrypted using the TLS encryption protocol.	No exceptions noted.
CC6.7.2	(Control 36) Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the enabled VPN encryption configurations to determine that encrypted VPNs were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.3	(Control 37) Employee workstations are configured with full disk encryption.	Inspected the enabled disk encryption configurations for a sample of current employee workstations to determine that employee workstations were configured with full disk encryption for each workstation sampled.	No exceptions noted.
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	(Control 38) Anti-malware software is installed on employee workstations and configured to scan registered endpoints in real time.	Inspected the enabled anti-malware software configurations for a sample of current employee workstations to determine that anti-malware software was installed on employee workstations and configured to scan registered endpoints in real time for each workstation sampled.	No exceptions noted.
CC6.8.2	(Control 31) Logging and monitoring systems are configured to collect data from in-scope production hosts to analyze potential security vulnerabilities based on criticality and to alert the security team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope production hosts to analyze security vulnerabilities based on criticality and to alert security team personnel when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC6.8.3	(Control 23) The ability to change SEV-1 and SEV-2 services production pipeline build configurations in the automated deployment tool is restricted to user accounts accessible by authorized personnel.	Inspected the pipeline operator member listings for a sample of in-scope product / service pipelines with the assistance of the manager of trust and governance to determine that the ability to change SEV-1 and SEV-2 services production pipeline build configurations in the automated deployment tool was restricted to user accounts accessible by authorized personnel for each service sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	(Control 31) Logging and monitoring systems are configured to collect data from in-scope production hosts to analyze potential security vulnerabilities based on criticality and to alert the security team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope production hosts to analyze security vulnerabilities based on criticality and to alert security team personnel when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC7.1.2	(Control 63) Logging and monitoring systems are configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC7.1.3	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC7.1.5	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	(Control 31) Logging and monitoring systems are configured to collect data from in-scope production hosts to analyze potential security vulnerabilities based on criticality and to alert the security team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope production hosts to analyze security vulnerabilities based on criticality and to alert security team personnel when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC7.2.2	(Control 63) Logging and monitoring systems are configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds were met and/or exceeded.	No exceptions noted.
CC7.2.3	(Control 20) A penetration test is performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding penetration testing remediation efforts to determine that a penetration test was performed by a third-party specialist on an annual basis to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the executive summary for the most recent penetration test performed and the remediation ticket for an example finding to determine that a penetration test was performed by a third-party specialist to identify threats and assess their potential impact to system security and availability and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.4	(Control 9) A vulnerability scanning tool is configured to run vulnerability scans on production hosts on at least a weekly basis. Security vulnerabilities that are detected are triaged and monitored through resolution via a ticketing system.	Inquired of the senior manager of security engineering regarding vulnerability scanning remediation efforts to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the vulnerability scan configurations, the results of an example scan generated during the period, and the remediation ticket for an example finding to determine that a vulnerability scanning tool was configured to run vulnerability scans on production hosts on at least a weekly basis and that security vulnerabilities that were detected were triaged and monitored through resolution via a ticketing system.	No exceptions noted.
CC7.2.5	(Control 10) A bug bounty program is utilized to identify and report vulnerabilities and threats. Security vulnerabilities that are detected are reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	Inquired of the manager of governance, risk, and compliance regarding bug bounty program remediation efforts to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team, triaged, and monitored through resolution via a ticketing system.	No exceptions noted.
		Inspected the bug bounty program overview and an example vulnerability ticket resolved during the period to determine that a bug bounty program was utilized to identify and report vulnerabilities and threats and that security vulnerabilities that were detected were reviewed by the product security team and triaged and monitored through resolution via a ticketing system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	(Control 24) Documented incident response policies and procedures are in place to guide personnel in documenting, identifying, containing, and remediating security incidents.	Inspected the security incident response playbook to determine that documented incident response policies and procedures were in place to guide personnel in documenting, identifying, containing, and remediating security incidents.	No exceptions noted.
CC7.3.2	(Control 41) A ticketing system is utilized by the security team to manage security incidents, response, and resolution. Details of the identification, containment, recovery, and communication are maintained within the ticketing system.	Inspected the ticket for a sample of incidents that occurred during the period to determine that a ticketing system was utilized by the security team to manage security incidents, response, and resolution and that details of the identification, containment, recovery, and communication were maintained within the ticketing system for each 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	(Control 24) Documented incident response policies and procedures are in place to guide personnel in documenting, identifying, containing, and remediating security incidents.	Inspected the security incident response playbook to determine that documented incident response policies and procedures were in place to guide personnel in documenting, identifying, containing, and remediating security incidents.	No exceptions noted.
CC7.4.2	(Control 41) A ticketing system is utilized by the security team to manage security incidents, response, and resolution. Details of the identification, containment, recovery, and communication are maintained within the ticketing system.	Inspected the ticket for a sample of incidents that occurred during the period to determine that a ticketing system was utilized by the security team to manage security incidents, response, and resolution and that details of the identification, containment, recovery, and communication were maintained within the ticketing system for each incident sampled.	No exceptions noted.
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	(Control 24) Documented incident response policies and procedures are in place to guide personnel in documenting, identifying, containing, and remediating security incidents.	Inspected the security incident response playbook to determine that documented incident response policies and procedures were in place to guide personnel in documenting, identifying, containing, and remediating security incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.2	(Control 41) A ticketing system is utilized by the security team to manage security incidents, response, and resolution. Details of the identification, containment, recovery, and communication are maintained within the ticketing system.	Inspected the ticket for a sample of incidents that occurred during the period to determine that a ticketing system was utilized by the security team to manage security incidents, response, and resolution and that details of the identification, containment, recovery, and communication were maintained within the ticketing system for each incident sampled.	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	(Control 48) OAR policies and procedures are in place to help guide personnel in requesting, documenting, and approving new products and services.	Inspected the documented OAR procedures to determine that OAR policies and procedures were in place to help guide personnel in requesting, documenting, and approving new products and services.	No exceptions noted.
CC8.1.2	(Control 65) The OAR process is required to be completed for new products and services assigned the following severity levels: • Severity one • Severity two	Inspected the OAR ticket for a sample of products and services added during the period to determine that the OAR process was required to be completed for new products and services assigned the following severity levels for each product / service sampled: • Severity one • Severity two	No exceptions noted.
CC8.1.3	(Control 47) A software development platform is used to centrally document, manage, and monitor change requests through implementation.	Inspected the listing of repositories within the software development platform to determine that a software development platform was used to centrally document, manage, and monitor change requests through implementation.	No exceptions noted.
CC8.1.4	(Control 39) The automated deployment tool is configured to require automated validation testing of SEV-1 and SEV-2 changes.	Inspected the automated deployment tool configurations for a sample of in-scope product / service pipelines to determine that the automated deployment tool was configured to require automated validation testing of SEV-1 and SEV-2 changes for each pipeline sampled.	No exceptions noted.
CC8.1.5	(Control 34) A monitoring tool is in place to log issues related to pipeline build configurations.	Inspected the monitoring tool configurations and an example alert generated during the period to determine that a monitoring tool was in place to log issues related to pipeline build configurations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.6	(Control 23) The ability to change SEV-1 and SEV-2 services production pipeline build configurations in the automated deployment tool is restricted to user accounts accessible by authorized personnel.	Inspected the pipeline operator member listings for a sample of in-scope product / service pipelines with the assistance of the manager of trust and governance to determine that the ability to change SEV-1 and SEV-2 services production pipeline build configurations in the automated deployment tool was restricted to user accounts accessible by authorized personnel for each service sampled.	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	(Control 57) Security management performs a risk assessment on at least an annual basis that considers the identification and assessment of risks arising from potential business disruptions. Identified risks are formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the identification and assessment of risks arising from potential business disruptions and that identified risks were formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies during the period.	No exceptions noted.
CC9.1.2	(Control 43) The risk management program includes the use of insurance to minimize the financial impact of cyber events.	Inspected the cyber insurance policy to determine that the risk management program included the use of insurance to minimize the financial impact of cyber events.	No exceptions noted.
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	(Control 58) Security management performs a risk assessment on at least an annual basis that considers the identification and assessment of risks associated with vendors and business partners. Identified risks are formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies.	Inspected the risk management policy and procedures and the most recent risk assessment documentation to determine that security management performed a risk assessment that considered the identification and assessment of risks associated with vendors and business partners and that identified risks were formally documented, analyzed, and reviewed by the audit committee along with mitigation strategies during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	(Control 19) Security personnel review third-party compliance reports and/or a completed security questionnaire as a component of the onboarding process for third-party service providers that store or access customer data.	Inspected the third-party risk management policy and the vendor security review documentation for a sample of vendors storing or accessing customer data that were onboarded during the period to determine that security personnel reviewed third-party compliance reports and/or a completed security questionnaire as a component of the onboarding process for each vendor sampled.	No exceptions noted.
CC9.2.3	(Control 30) The company obtains and makes available to customers the most recently completed third-party compliance certifications, including physical and environmental controls, for the company's colocation data centers.	Inspected the listing of in-scope data center colocation facilities and the data center compliance certification matrix on the company's website to determine that the company obtained and made available to customers the most recently completed third-party compliance certifications, including physical and environmental controls, for the company's colocation data centers.	No exceptions noted.

Additional Criteria for Availability

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0 - Additional Criteria for Availability			
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	(Control 63) Logging and monitoring systems are configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds were met and/or exceeded.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	(Control 63) Logging and monitoring systems are configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds are met and/or exceeded.	Inspected the logging and monitoring system dashboard, alerting configurations, and registered hosts and an example alert generated during the period to determine that logging and monitoring systems were configured to collect data from in-scope systems to analyze resource utilization and system performance based on criticality and to alert the CloudOps team when predefined thresholds were met and/or exceeded.	No exceptions noted.
A1.2.2	(Control 33) Business continuity and disaster recovery plans are in place and are reviewed on an annual basis.	Inspected the business continuity and disaster recovery plans and most recent tabletop exercise performed to determine that business continuity and disaster recovery plans were in place and were reviewed during the period.	No exceptions noted.
A1.2.3	(Control 64) The engineering team dedicated to platform availability and resiliency meets on a weekly basis to review incident trends, post-incident reviews (PIR), and action items affiliated with PIRs which considered the time to detect, severity, root cause, impact on availability, and customer impact of incidents.	Inspected the recurring operational review meeting invite, listing of attendees, and agenda overview to determine that the engineering team dedicated to platform availability and resiliency met on a weekly basis to review incident trends, PIRs, and action items affiliated with PIRs which considered the time to detect, severity, root cause, impact on availability, and customer impact of incidents.	No exceptions noted.
CSOC.02	Colocation data centers are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.		
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	(Control 33) Business continuity and disaster recovery plans are in place and are reviewed on an annual basis.	Inspected the business continuity and disaster recovery plans and most recent tabletop exercise performed to determine that business continuity and disaster recovery plans were in place and were reviewed during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.2	(Control 64) The engineering team dedicated to platform availability and resiliency meets on a weekly basis to review incident trends, post-incident reviews (PIR), and action items affiliated with PIRs which considered the time to detect, severity, root cause, impact on availability, and customer impact of incidents.	Inspected the recurring operational review meeting invite, listing of attendees, and agenda overview to determine that the engineering team dedicated to platform availability and resiliency met on a weekly basis to review incident trends, PIRs, and action items affiliated with PIRs which considered the time to detect, severity, root cause, impact on availability, and customer impact of incidents.	No exceptions noted.