DigitalOcean
System and Organization Controls 2 Report

Description of DigitalOcean’s Cloud Infrastructure Platform

Throughout the period January 1, 2020 to November 30, 2020
with Independent Service Auditor’s Report

DigitalOcean

System and Organization Controls 2 Report
Description of DigitalOcean's Cloud Infrastructure Platform

Throughout the period January 1, 2020 to November 30, 2020

Table of Contents

DigitalOcean’s Cloud Infrastructure Platform Management Assertion

February 24, 2021

We have prepared the accompanying Description of DigitalOcean’s Cloud Infrastructure Platform (Description) of DigitalOcean (Service Organization) in accordance with the criteria for a description of a service organization’s system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (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 from interactions with the System throughout the period January 1, 2020 to November 30, 2020, particularly information about system controls that the Service Organization has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for Security and Availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

DigitalOcean uses Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite to provide data center hosting for DigitalOcean products and services. The Description includes only the controls of DigitalOcean and excludes controls of Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite. The Description also indicates that certain trust services criteria specified therein can be met only if Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite’s controls assumed in the design of DigitalOcean’s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of DigitalOcean’s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

a. The Description presents the System that was designed and implemented throughout the period January 1, 2020 to November 30, 2020, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of DigitalOcean’s controls throughout the period January 1, 2020 to November 30, 2020.

c. The DigitalOcean controls stated in the Description operated effectively throughout the period January 1, 2020 to November 30, 2020 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of DigitalOcean’s controls throughout the period January 1, 2020 to November 30, 2020.

Building a better
working world

Ernst & Young LLP
710 Bausch & Lomb Place
Rochester, NY 14604-2704

Tel: +1 585 987 4600
Fax: +1 585 987 4675
ey.com

Independent Service Auditor’s Report

Management of DigitalOcean

Scope
We have examined DigitalOcean’s accompanying Description of DigitalOcean’s Cloud Infrastructure Platform of its Cloud Infrastructure Platform system for providing cloud services throughout the period January 1, 2020 to November 30, 2020 (Description) in accordance with the criteria for a description of a service organization’s system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period January 1, 2020 to November 30, 2020 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for Security and Availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

DigitalOcean uses Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite (subservice organizations) to provide data center hosting for DigitalOcean products and 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 system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite. Our examination did not extend to the services provided by Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite and we have not evaluated whether the controls management assumes have been implemented at Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2020 to November 30, 2020.

The Description also indicates that DigitalOcean’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of DigitalOcean’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

DigitalOcean’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 the service commitments and system requirements were achieved. DigitalOcean has provided the accompanying assertion titled, DigitalOcean’s Cloud Infrastructure Platform Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service

commitments and system requirements would be achieved based on the applicable trust services criteria. DigitalOcean is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization’s service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

Service auditor’s responsibilities
Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization’s service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization’s service commitments and system requirements

- performing procedures to obtain evidence about whether the controls stated in the Description are 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.

- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.

- testing the operating effectiveness of those controls based on the applicable trust services criteria.

- evaluating the overall presentation of the Description.

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

Inherent limitations
The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization 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 evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls
The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests and Results of Test (Description of Tests and Results).

Opinion
In our opinion, in all material respects:

a. the Description presents the Cloud Infrastructure Platform system that was designed and implemented throughout the period January 1, 2020 to November 30, 2020 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if the subservice organizations and user entities applied the controls assumed in the design of DigitalOcean’s controls throughout the period January 1, 2020 to November 30, 2020.

c. the controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period January 1, 2020 to November 30, 2020, if the subservice organization and user entity controls assumed in the design of DigitalOcean’s controls operated effectively throughout the period January 1, 2020 to November 30, 2020.

Restricted use
This report, including the description of tests of controls and results thereof in the Description of Tests and Results, 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 January 1, 2020 to November 30, 2020 and prospective user entities, independent auditors and practitioners providing services to such user entities 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, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization’s controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks

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

Ernst + Young LLP

February 24, 2021
Rochester, New York

Description of DigitalOcean’s Cloud Infrastructure Platform

Company Overview

Founded in 2012 based in New York, DigitalOcean provides a cloud platform to deploy, manage, and scale applications of any size, removing infrastructure friction and providing predictability.

DigitalOcean provides their customers with a user interface and application programming interface (API), a robust set of features, thousands of tutorials, and a library of open source resources.

Boundaries of the System

Included within the scope of this report are the infrastructure, software, people, procedures, and data supporting the DigitalOcean production environment. DigitalOcean offers Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) services. Capabilities are delivered through a browser-based web application and via API.

Infrastructure

Products are hosted exclusively on DigitalOcean’s platform. DigitalOcean operates an IaaS and PaaS Cloud hosting platform within highly-available data centers around the world.

IaaS products include Droplets, Block Storage, and Spaces. A droplet is a virtual machine that is allocated resources, such as central processing unit (CPU), Random-Access Memory (RAM), and disk storage, from a physical host. A hypervisor makes sure that the multiple Droplets running on a physical host each receive their virtual resources. Block storage volumes are network-based block devices that provide additional data storage for Droplets. Spaces is a bucket to store and serve files.

PaaS products include Kubernetes, Managed Databases, App Platform, and Container Registry. These products provide virtualized environments where the infrastructure is pre-configured so that developers can focus on building their code.

DigitalOcean also provides additional features of the core products. Marketplace allows for one-click applications that create a Droplet and configures it with a service of the customer’s choosing. Other additional features include Images, Networking Services, and Projects features to help manage virtualized infrastructure.

DigitalOcean products and services are all virtualized which means that the disks, hypervisors, and load balancers can scale to meet the demand as a cloud provider more efficiently. As such, this requires highly available hardware and DigitalOcean monitors continuously for outages and failures.

Data Centers

DigitalOcean utilizes a number of co-located data center providers to host DigitalOcean products and services. DigitalOcean data centers house the various physical firewalls, switches, load balancers, routers, servers, and disks that store or transmit DigitalOcean data, application code, and related system monitoring utilities.

Each data center is responsible for the physical and environmental controls in this environment. DigitalOcean personnel have physical access to the co-located data centers as required.

DigitalOcean utilizes data centers which operate in geographically separated locations to provide lower latency network links and higher availability for customers. The regions in which DigitalOcean's data centers are located include:

- San Francisco, United States
- New York City, United States
- Toronto, Canada
- London, United Kingdom
- Amsterdam, Netherlands
- Frankfurt, Germany
- Bangalore, India
- Singapore

People

The personnel primarily involved in the security governance, operation, and management of DigitalOcean include the following:

- *Security* – Responsible for creating policies, standards, and procedures that relate to and enforce the risk, governance, privacy, and compliance posture of the organization

- *Engineering/Product* – Responsible for designing, building, and maintaining products while adhering to data protection, privacy, and security standards

- *Information Technology (IT)* – Responsible for workplace experience, employee asset management, and employee account lifecycle management

- *People (HR)* – Responsible for talent acquisition, talent strategy, and total rewards

- *Legal* – Responsible for general counsel operations and external facing policies and terms

- *Finance* – Responsible for budgeting and finance operations

- *Customer Success and Support* – Responsible for assisting customers with software usage issues

- *Communications* – Responsible for reviewing internal and external communication

Vendor Agreements

Vendor agreements, including any security and availability commitments, are reviewed by DigitalOcean management during the procurement process. Prior to services rendered, the vendor and DigitalOcean are required to sign the vendor agreement terms and conditions. DigitalOcean management performs vendor security review procedures over third- party service providers who store or access customer data prior to engaging the third party and annually thereafter.

Procedures

DigitalOcean maintains a set of internal policies, standards, and procedures to operate the DigitalOcean systems. These documents are developed to provide employees with guidance and to reinforce the commitment to data privacy and data protection. DigitalOcean defines policies, standards, and procedures as:

- Policies – Policies address an issue or topic at a broad level, usually encompassing the entire organization and its commitment to adherence.
- Standards – Standards offer an ideal state for a particular issue or topic. Exceptions to a standard are accepted only if such deviation is discussed, agreed upon, documented, and acknowledged at the team level.
- Procedures – Procedures are detailed step-by-step processes. They are typically living documents owned and updated at the team level and often referenced in a policy or standard.

Data

DigitalOcean provides details on the customer data that is collected, reasons for collection, and use of the data within the company's Terms of Service and Privacy Policy. DigitalOcean employs a variety of security technologies and measures designed to protect information from unauthorized access, use, or disclosure.

The DigitalOcean environment includes the following data:

1. Information Customers Provide:
   a. Account Registration
   b. Payment Information
   c. User Content
   d. Additional information provided by the customer
2. Information Collected when Customers use DigitalOcean Services (Cookies and other tracking technologies)
3. Information Received from Third-Parties linked with customer's services

Description of the Control Environment, Information and Communication, Monitoring, and Risk Assessment Processes

Control Environment

The following control framework encompasses DigitalOcean's efforts to establish and maintain an environment that supports the effectiveness of specific controls.

A company's control environment reflects the overall attitude, awareness, and actions of executive management, the board of directors, and other stakeholders concerning the importance of controls and the emphasis given to controls in the company's policies, standards, procedures, and organizational structure. The following is a description of the control environment as it pertains to the DigitalOcean systems.

Control Activities

Customer Success and Support

DigitalOcean's mission is to accelerate the success of developers and teams on the company's platform through strong technical and best practice guidance, while making sure that the company's products meet the high expectations of customer communities.

DigitalOcean's Customer Success & Support (CSS) team assists customers through their business journey by enabling them to find and use resources to fully utilize the DigitalOcean platform. The CSS team further acts as the frontline for customer communications and inquiries that range from general questions to technical support of DigitalOcean services.

Product Development and Delivery

Products are developed at DigitalOcean via a defined Product Development Life Cycle that includes a set of artifacts and milestones to be used during the development of products and services to help ensure that products are built effectively, efficiently, and transparently. The steps of that lifecycle are Opportunity Assessment, Discovery, Planning, Delivery, General Availability, and Retirement. There are subtasks that include approval, testing, and validation by engineering and security teams. Products maintain product managers that support the product development lifecycle.

Information Technology

DigitalOcean's IT team supports employees and contractors, providing access and technical support for all company-issued hardware and software. The team also maintains the company's IT Infrastructure in all company offices and are admins for a number of software and services that employees utilize. Additionally, the team works with the security team to coordinate onboarding and offboarding for DigitalOcean's employees and external contractors worldwide.

People Team

DigitalOcean's job-posting process requires all positions to go through a series of approvals prior to posting on the Careers webpage. Job postings are a collaboration of the internal recruiter and hiring manager. Employment candidates undergo a vetting process to evaluate their competency, qualifications, and experience. This process includes an assessment of the candidate's qualifications and an interview with management and relevant team members to determine whether the candidate meets the documented job requirements. Candidate information is captured in an applicant tracking system, and feedback and interview notes are captured within the candidate's profile. DigitalOcean performs background checks on full-time new hires.

Upon starting, employees go through an onboarding process which includes product training, security training, meetings with senior leadership, and team-specific onboarding.

DigitalOcean has an organizational chart which defines reporting lines. To help ensure the various organizations at DigitalOcean know their security obligations, DigitalOcean defines job descriptions outlining roles and responsibilities. These job descriptions are made available to employees to enable awareness of their responsibilities and commitments to the security of internal systems and customer data. Further, DigitalOcean maintains an employee security training program to help ensure employees are aware of their individual responsibilities and commitments to data privacy and data protection. New employees and contractors receive security awareness training upon hire and receive specialized security training as needed for their role.

DigitalOcean managers perform a semi-annual performance review as well as regular one-on-one meetings with each of their direct reports to evaluate the employees' competency and skills to fulfill job responsibilities.

Monitoring

Management Oversight

Annually, DigitalOcean monitors the effectiveness of its key internal controls through performance of an internal risk assessment. The results of this assessment are shared with senior management, tracked, and remediated in accordance with the Risk Assessment/Audit Policy. Additionally, relevant security policies, standards, and procedures are regularly reviewed for relevance and effectiveness and are approved by Security Leadership.

Security Monitoring

Security Incidents are managed by a dedicated Security Operations Center (SOC) team that follows a detailed Security Incident Response Cycle which includes: Identification, Containment, Eradication, Recovery, and Retrospection and Preparation. Each phase of the cycle includes specific tasks and actions that are performed to help ensure that the steps are taken at each phase, including:

- Identification – Confirmation of initial indicators and declaration of a security incident
- Containment – Investigation, isolation, and scoping of impacted systems, users, resources, or data
- Eradicate – Removal of access, tools, accounts, etc. to limit the spread of impact
- Recover – Restoration and recovery of affected systems back to normal operations

- Retrospective – Documentation, discussion of post-incident lessons learned, root-cause determination, and recommendations to deter a future incident

- Preparation – Helping ensure staff are trained, tools and software are available, and related services are ready for future incidents

Sub-Service Organization Monitoring

DigitalOcean utilizes co-located data center providers to host DigitalOcean products and services and their physical security controls are regularly audited and assessed for compliance and effectiveness through System and Organization Control Reports, which are reviewed by the company.

Risk Assessment

An entity's risk assessment process is its identification, analysis, and management of risks in its service delivery to user organizations. DigitalOcean recognizes that risk management is a critical component of its operations that helps verify customer data is protected. DigitalOcean incorporates risk management throughout its processes at both the corporate and business segment levels.

DigitalOcean has a defined risk management process to identify and manage risks that may affect the system's security or wider business operations. The Risk Assessment/Audit Policy defines risk tolerances and includes details of the identification, analysis, communication, and mitigation of risks relating to company operations, safeguarding of informational assets, fraud, financial performance and changes in technology or client relationships. DigitalOcean's Security leadership performs a yearly risk assessment to identify and evaluate potential threats to the effectiveness of the control environment. Additionally, ongoing risks and security issues are continually maintained and updated by the Security team to help ensure they are continually identified, tracked, and mitigated based on magnitude and frequency. Fraud-related risks to DigitalOcean are regularly monitored by a dedicated Abuse Operations team and reviewed with Security Leadership.

Management is responsible for implementing procedures to identify the risks inherent in DigitalOcean's operations and for implementing procedures to monitor and mitigate these risks. The foundation of this process is management's knowledge of its operations, and its close working relationship with its customers and vendors.

In addition, to help further mitigate its risk, DigitalOcean maintains an insurance policy against cybersecurity-related loss events.

Information and Communication

To help align DigitalOcean business strategies and goals with operating performance, management is committed to maintaining effective communication both with employees and customers. DigitalOcean regularly performs training sessions and Company All-Hands meetings. Concerns or feedback can be submitted for responses by the executive team during Company All-Hands meetings.

Criteria and Controls

Physical and Information Security

To help secure DigitalOcean's employees, customers, and the data it processes and stores, defense-in-depth layers of physical and information security controls have been implemented. DigitalOcean maintains access control policies and procedures as well as documented access request procedures to enforce role-based access control (RBAC).

Password Controls

Passwords for applications and tools that impact DigitalOcean's production environment are managed via Secrets Authentication tooling that includes key management. Employees sign onto the DigitalOcean VPN using multi-factor authentication and a complex password. Customer passwords are securely encrypted and unavailable for employees to access.

Customers are responsible for keeping passwords from being disclosed to unauthorized parties. Customers must choose passwords with sufficient entropy and have the option of using multi-factor authentication.

Network Access

Internal DigitalOcean network access is controlled at each boundary layer by multiple controls. To access internal services necessary for the normal course of daily activities, DigitalOcean employees must be authenticated to a general VPN profile. This VPN access is even mandated for employees within DigitalOcean office space. Access to more sensitive DigitalOcean systems requires a more restrictive VPN profile that is access controlled. Employees must be explicitly approved to this profile by their management. All VPN access is controlled by two factor authentication (2FA) and user behavior analytics.

DigitalOcean restricts remote access to its internal network and systems based on documented policies and through an encrypted VPN connection.

New User Access

New DigitalOcean employees, interns, or contractors have access provided to them based on the company's Access Control Policy. Access is granted based on business justification, with the asset owner's authorization and limits based on "need-to-know" and "least privilege" principles. Additionally, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.

Departmental Changes/Modified User Access

Users who change roles have their access permissions reviewed and modified as needed. Access is provided on a need-to-know basis and is reviewed according to the DigitalOcean Access Control Policy.

Termination/Removal of User Access

Automated procedures are in place to disable user accounts upon the user’s leave date. Access permissions are reviewed and modified as needed during both a change in role and termination.

Vulnerability Management

DigitalOcean contracts with independent assessors to perform penetration testing of the DigitalOcean boundary on a regular basis. The independent assessors use accepted industry standard penetration testing methodologies. Identified vulnerabilities and risks are tracked and remediated accordingly by the Security team.

DigitalOcean’s vulnerability management program looks at the company’s entire IT environment (hardware, infrastructure, product).

At the hardware level, DigitalOcean works with chipset manufacturers to get access to vulnerability fixes prior to disclosure to the general public.

At the infrastructure level DigitalOcean continuously scans the company’s fleet of servers for vulnerabilities at the firmware, operating system, and application level, allowing for timely identification of software vulnerabilities.

At the product level, DigitalOcean conducts product security reviews during design and development to identify security issues early and remedy them prior to product release.

In addition to contracted independent assessors, DigitalOcean participates in a HackerOne Vulnerability Disclosure Program and Bug Bounty Program designed to engage the security research community and surface vulnerabilities of the company’s external boundary and products. Customers can report security vulnerabilities or issues through the company’s Security Contacts Page.

Vulnerabilities identified within the IT environment (as mentioned above) are triaged, tracked, handed off to IT/business to remediate and resolve in accordance with the context of the risk they present.

Malware Protection

The DigitalOcean Security group responds to malicious events, including escalating and engaging specialized support groups. A number of key security parameters are monitored to identify potentially malicious activity on the systems. DigitalOcean utilizes SentinelOne as its endpoint protection and anti-virus software which is installed on every employee’s machine and monitors for malicious activity 24/7. If malicious software or activity is detected, the Security team is alerted and the anomaly is dealt with in accordance with documented incident management procedures.

Information in transit, including user authentication information and transmission of private or confidential information through DigitalOcean, is encrypted using Secure Sockets Layer (SSL) over Hypertext Transfer Protocol Secure (HTTPS) connections.

Additionally, DigitalOcean Security also utilizes GreatHorn for email security and phishing campaign management.

Physical Security

DigitalOcean's platform is hosted within multiple datacenter provider facilities. DigitalOcean reviews the System and Organization Controls reports on an annual basis for completeness, accuracy, and relevance to DigitalOcean's business needs. Any questions or concerns in regard to the hosted facility SOC 2 report are followed-up and tracked to resolution on a timely basis.

System Implementation and Change Management

Software Development Life Cycle (SDLC) Overview

DigitalOcean's SDLC integrates information security from product and service design. Continual integration of security practices in DigitalOcean's SDLC enables early identification and mitigation of security vulnerabilities and misconfigurations; awareness of potential software coding challenges caused by required security controls; identification of shared security services and continued evaluation of services based on Open Web Application Security Project (OWASP) standard criteria, which improves security posture through proven methods and techniques; and enforces DigitalOcean's already comprehensive risk management program.

SDLC Process

DigitalOcean utilizes a combination of Continuous Integration and Continuous Delivery (CI/CD) and traditional SDLC processes for software development. CI/CD allows development teams to deliver code changes more frequently and reliably. This frequency allows teams to incrementally improve production code, identify defects quicker, and streamlines the editing and process. For larger product and software deployments, DigitalOcean utilizes its SDLC process with phases defined as:

- Discovery – Engineering teams at DigitalOcean gather, assess, prototype, and refine requirements for new projects.
- Planning – Teams develop project and resource plans as well as bring the Security team for initial review and planning.
- Implementation – Teams perform iterative development with continued support and input from the Security team throughout. Code reviews, testing, Quality Assurance (QA), and additional adjustments are made during this phase prior to deployment.
- Deployment – The ability to deploy code, configuration, or infrastructure changes to production is restricted to designated personnel.
- Maintenance – Deployments are monitored to help ensure the changes are not negatively affecting the overall performance or health of the service or application.

Feature Enhancement

For new feature enhancements to existing services or systems running in production, DigitalOcean development teams follows a step-by-step process:

- Ticket Creation – A developer or team completes a ticket with detailed information regarding feature addition.

- Development – Identification of the effort required, development of feature update, and security evaluation is performed.
- Test – Manual and automated testing is performed by the developer or team member and is further reviewed by Security for pre-production.
- Deploy – Approved changes to the system follow the Engineering Change Management Standard and additional post-deployment testing is performed for continuous monitoring and improvement.

Bug Fixes

When an existing DigitalOcean service or system that is in production requires bug fixes, the developer or development team follows the Bug Fixes process:

- Ticket Creation – A developer or team completes a ticket with detailed information regarding the bug identified, impact, and fix required.
- Bug Fix – Developer or team reproduces the problem, fixes it, and Security reviews (for Major Changes only).
- Bug Test – Developer or team tests the bugfix and again involves Security for review (for Major Changes only).
- Deploy – The developer or team deploys approved changes following the Engineering Change Management Standard and additional post-deployment testing is performed for continuous monitoring and improvement.

Change Management Overview

DigitalOcean maintains a Change Management Policy which documents the overall methods and principles that govern how the company documents, develops, tests, approves, and deploys software.

Change Management Procedures

DigitalOcean services have developed formal standard operating procedures (SOPs) governing the change management process. These SOPs cover both software development and hardware change and release management, and are consistent with established regulatory guidelines. The company utilizes GitHub Enterprise as the source code repository across the organization.

Change Exemptions

Changes defined as routine maintenance are not required to strictly adhere to the Change Management Policy. These changes present low risk and low impact and are known changes in the environment. All other exceptions must be requested from the system owner and reviewed by senior management with a detailed explanation and business justification.

Emergency Changes

Emergency changes follow an expedited process, meaning that change management controls are still adhered to. Any changes that require emergency deployments will still be reviewed and tested; however final approvals may be obtained after the deployment of the change.

Change Management Monitoring

DigitalOcean employs service-oriented architecture to support the infrastructure that runs the virtualized products. Services are monitored continuously for anomalous behavior based on the services severity scale rating. For pushing code changes, DigitalOcean employs a Continuous Integration/Continuous Deployment pipeline that encourages many minimal code changes to prevent and detect code failures.

For major changes, DigitalOcean follows an Operational Acceptance Review completed by the Cloud Operations team that includes smoke testing, which tests the stability of deployed code, as well as review from Security and Cloud Operations to validate that any changes have monitoring and support. All services and changes deployed that are production impacting include service uptime alerting and are engineered to monitor the impact of the change rather than code change itself.

Operations Monitoring and Problem Management

Network System and Device Monitoring

Proactive monitoring continuously measures the performance of key subsystems of the DigitalOcean services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. Service interruptions, performance degradation, scheduled maintenance, or other issues affecting customers are communicated via a status page, email, or application notification.

The Security team uses intrusion detection software (IDS) software to identify, monitor, and evaluate security threats and unusual system activity. Alerts are sent to Security personnel for items that have exceeded predefined thresholds and are tracked to resolution.

Vulnerability assessment and scanning tools are specifically designed to operate in virtualized environments. Procedures have been established and implemented to scan for vulnerabilities on DigitalOcean managed hosts in the scope boundary. DigitalOcean implements vulnerability scanning on server operating systems, databases, and network devices. The vulnerability scans are performed on a regular basis.

System Backup

Device Backup and Monitoring

DigitalOcean backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Backup standards and policies, procedures and controls are verified, documented and audited both internally and by third party assessors.

Environmental Safeguards

DigitalOcean data centers have a number of physical and environmental controls in place to protect data and services from unauthorized access as well as environmental threats. These controls are performed by third parties and monitored by DigitalOcean to determine compliance.

Complementary User Entity Controls

DigitalOcean's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to DigitalOcean's services to be solely achieved by DigitalOcean control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of DigitalOcean's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgement in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for ensuring the supervision, management, and control of the use of DigitalOcean's services by their personnel. Relevant Criteria: CC 1.0

2. User entities are responsible for understanding and complying with their contractual obligations to DigitalOcean. Relevant Criteria: CC 2.0

3. User entities are responsible for immediately notifying DigitalOcean of any actual or suspected security breaches, including compromised user accounts. Relevant Criteria: CC 2.0

4. User entities are responsible for the security and privacy of the contents of their droplets. Relevant Criteria: CC 6.0

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. Relevant Criteria: CC 6.0

6. User entities are responsible for maintaining their own system of record. Relevant Criteria: CC 7.0

7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize DigitalOcean services. Relevant Criteria: CC 9.0

Complementary Subservice Organization Controls

DigitalOcean’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to DigitalOcean’s services to be solely achieved by DigitalOcean control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of DigitalOcean.

The following subservice organization controls should be implemented by Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization – Equinix, Digital Realty, Interxion, NTT Communications, and CoreSite	
Control Area	**Control Activity Description**
Physical Security	Physical access to data centers is approved by an authorized individual.
	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
	Physical access points to server locations are recorded by closed circuit television camera (CCTV).
	Physical access points to server locations are managed by electronic access control devices.
	Physical access to assets is removed only after the ability to read or recover data and software from those assets has been diminished.
Environmental Security	Data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in data centers.
	Data centers are protected by fire detection and suppression systems.
	Data centers have generators to provide backup power in case of electrical failure.
Information Security Monitoring	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	Data centers perform periodic reviews to validate adherence with security and operational standards.

DigitalOcean management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet the relevant trust services criteria through written contracts, such as service level agreements. In addition, DigitalOcean performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Description of Criteria, Controls, Tests and Results of Tests

Controls to Meet the Trust Services Criteria

On the pages that follow, the controls to meet the applicable trust services criteria have been specified by, and are the responsibility of, DigitalOcean. The testing performed by EY and the results of tests are the responsibility of the service auditor.

The full text of the trust services criteria for the security (also referred to as common criteria) and availability principles are contained in the testing tables for each criterion. This section describes the controls at DigitalOcean that achieve the applicable trust services criteria.

Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity (IPE)

For tests of controls requiring the use of IPE, procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE produced by DigitalOcean and provided to user entities, IPE used by DigitalOcean management in performance of controls (e.g., periodic review of user listings), and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures were performed to address the completeness and accuracy of the data or reports used: (1) inspect source documentation relating to the IPE; (2) inspect the query, script, or parameters used to generate the IPE; (3) agree data between the IPE and the source; and/or (4) inspect the IPE for anomalous gaps in sequence or timing.

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC1.0 – Criteria Related to Control Environment		
CC 1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**(Control 1)**: Senior Management's commitment to implementing, maintaining, and continually improving the security risk posture includes implementation of an Acceptable Use Policy, Employee Handbook, and Employee Security Training.	Inspected the most recent version of the Acceptable Use Policy and Employee Handbook and determined for a sample of new hire employees that each employee completed the mandatory security training. **No deviations noted.**
	(Control 2): Employees receive performance evaluations semi-annually to evaluate the employee's competency and skills to fulfill job responsibilities.	Inspected the semi-annual performance evaluations for employees and evidence that the mid-year review process was successfully completed and that each employee received a performance review for the previous six months. **No deviations noted.**
CC 1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**(Control 44)**: The board of directors is comprised of directors who are independent of DigitalOcean's operations.	Inspected DigitalOcean's Board of Directors (BOD) and determined that they are independent of DigitalOcean's operations. **No deviations noted.**
	(Control 45): Quarterly, the DigitalOcean executive team meets with the board of directors to review financial and operational performance and risks to the business.	Inspected a sample of Board of Directors meeting minutes and determined that financial and operational performance, including internal control, and risks to the business were discussed. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**(Control 4)**: DigitalOcean has an organizational chart that defines reporting lines.	Inspected the organization reporting hierarchy and determined that reporting lines were formally defined and managed. **No deviations noted.**
	(Control 6): DigitalOcean maintains written policies and procedures related to Security and makes this documentation available to relevant internal employees and contractors.	Inspected policies related to Security (Information Risk Management Policy, Information Security Risk Management Procedure, Data Protection Policy, Access Control Policy and Access Control Procedure) and determined that DigitalOcean Security policies are communicated and available to employees and contractors. **No deviations noted.**
CC 1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**(Control 7)**: The Security Team is evaluated based on an extensive interview process which assesses experience, training, and education. Each person's skill sets are aligned with their role and responsibilities. In order to obtain new skills and stay abreast of industry best practices team members utilize the organization's education reimbursement benefit to attend security conferences, trainings, and are also members of professional associations.	Inspected the security team's conference and education reimbursement form, DigitalOcean's learning and development resources page, and the recruiting process followed, and determined that DigitalOcean follows an extensive interview process and encourages its security team members to obtain new skills and stay abreast of industry best practices. **No deviations noted.**
CC 1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**(Control 5)**: DigitalOcean defines job descriptions outlining roles and responsibilities, including those related to its requirements and commitments. Job descriptions are made available to enable employee awareness of their responsibilities.	Inspected a sample of job descriptions and determined that the descriptions posted by DigitalOcean contain job responsibilities and a list of requirements considered for the positions. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC2.0 – Criteria Related to Communication and Information Criteria		
CC 2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**(Control 8)**: Management performs an annual assessment of key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements. Results are shared with senior management, tracked, and remediated in accordance with the Risk Assessment Policy.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization and that key risks were identified with potential remediating actions proposed. Inspected a sample Board of Directors meeting minutes and determined that key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements were discussed. **No deviations noted.**
	(Control 9): The Security team performs weekly internal (production) and external vulnerability scans. Identified vulnerabilities are analyzed, tracked, and resolved according to the Vulnerability Management Policy.	Inspected the active scans report and determined that internal and external scans are run on infrastructure supporting DigitalOcean's Cloud Infrastructure platform at least weekly. Inspected a sample of vulnerability scans and associated scan results and determined that each ran timely and that findings were identified, tracked, and monitored/resolved. **No deviations noted.**
	(Control 10): A Bug Bounty Program is employed to utilize community driven vulnerability and bug hunting. Identified vulnerabilities are analyzed, tracked, and resolved according to the Bug Bounty Evaluation Program.	Inspected evidence to support DigitalOcean's use and participation in a Bug Bounty Program. Inspected a sample of vulnerabilities found through the program and determined that DigitalOcean analyzes, tracks, and resolves the identified vulnerabilities. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**(Control 6)**: DigitalOcean maintains written policies and procedures related to Security and makes this documentation available to relevant internal employees and contractors.	Inspected policies related to Security (Information Risk Management Policy, Information Security Risk Management Procedure, Data Protection Policy, Access Control Policy and Access Control Procedure) and determined that DigitalOcean Security policies are communicated and available to employees and contractors. **No deviations noted.**
	(Control 11): Appropriate documentation and communication channels are available to employees to report security incidents.	Inspected the DigitalOcean Incident Response Playbook, along with other Security and Incident Response policies, and determined that the policy outlines the necessary stages of incident response for security incidents. Inspected a sample of security incidents, including screenshots of the security alerts and associated tickets, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**
CC 2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**(Control 12)**: Customers and External Parties acknowledge and agree to DigitalOcean's Terms of Service and Privacy Policy prior to using the services. These policies include information related to system design and operation, system boundaries, system security, support functions, and responsibilities.	Inspected the Terms of Service Agreement and Privacy Policy and determined that a user agrees to these policies by signing up for DigitalOcean's services. In addition, the policies include information related to system design and operation, system boundaries, system security, support functions, and responsibilities. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 2.3 (continued)	**(Control 13)**: Customers receive notification of material changes to the Terms of Service and Privacy Policy. In addition, significant changes to application functionality are communicated to customers via email or through the application after the implementation of the change.	Inquired of Management and determined that updates to the Terms of Service and Privacy Policy are made available on the company website. Inspected the public DigitalOcean website and determined that the documentation is readily available under the Legal section of the site, allowing customers access at any time to review the policies. **No deviations noted.**
	(Control 14): Service interruptions, performance degradation, scheduled maintenance, or other issues affecting customers are communicated via a status page, email, or application notification.	Inspected policies and documentation surrounding service interruptions, performance degradation, scheduled maintenance and the Infrastructure Operations team and determined that there are procedures in place to relay messages of this nature to customers. Inspected a sample of service interruptions, performance degradations, and scheduled maintenance on the public DigitalOcean status page along with associated tickets opened and determined that customers were notified of any significant issues that would potentially affect DigitalOcean products. **No deviations noted.**
	(Control 15): DigitalOcean's website includes contact information for support and a link to its disclosure policy which provides external users with information on how to responsibly report identified security vulnerabilities.	Inspected DigitalOcean's website and determined that there are links for customers and other external users to report and contact DigitalOcean for identified security vulnerabilities or suspicious activities. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC3.0 – Criteria Related to Risk Assessment		
CC 3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**(Control 16)**: Senior management maintains a Risk Assessment/Audit Policy that defines risk tolerances and includes the identification, analysis, communication, and mitigation of risks relating to the company operations, safeguarding of informational assets, and changes in technology.	Inspected the Information Security Risk Management policy and determined that it includes processes on the identification, analysis, communication, and mitigation of risks relating to the company operations, safeguarding of informational assets, and changes in technology. **No deviations noted.**
CC 3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**(Control 17)**: DigitalOcean Security management performs an annual risk assessment to identify, evaluate, and track identified risks, including those related to fraud and the security of customer data. Based on the determined magnitude and frequency, controls are put in place to mitigate risks.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization including fraud and security and that key risks were identified with potential remediating actions proposed. **No deviations noted.**
	(Control 18): The Security team maintains a business risk matrix, which tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities.	Inspected the 2020 Business Risk tracker which identifies the key risks to the business. Additionally, inspected the 2020 Risk Register which tracks each risk, risk mitigation plans and current risk mitigation status. **No deviations noted.**
CC 3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**(Control 46)**: Fraud-related risks to DigitalOcean are regularly monitored with a dedicated Abuse Operations team and reviewed with Security Leadership.	Inspected system-generated evidence showing monthly generated and ongoing fraud-related risk logs and determined that the risks are regularly monitored. Inspected notifications and corresponding tickets pertaining to the identified risks and determined that fraud-related risks are regularly reviewed by the Abuse Operations team and Security Leadership. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**(Control 17)**: DigitalOcean Security management performs an annual risk assessment to identify, evaluate, and track identified risks, including those related to fraud and the security of customer data. Based on the determined magnitude and frequency, controls are put in place to mitigate risks.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization including fraud and security and that key risks were identified with potential remediating actions proposed. **No deviations noted.**
	(Control 18): The Security team maintains a business risk matrix, which tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities.	Inspected the 2020 Business Risk tracker which identifies the key risks to the business. Additionally, inspected the 2020 Risk Register which tracks each risk, risk mitigation plans and current risk mitigation status. **No deviations noted.**
	(Control 19): DigitalOcean management performs vendor security review procedures over third-party service providers who store or access customer data prior to engaging the third party and annually thereafter.	Inspected system-generated evidence of Vendor Security Reviews performed within the period of this report and determined security related risks of each vendor were evaluated prior to contract commencement. Inspected a sample of Vendor Security Reviews and determined that each review consisted of a security review and a legal/contract review. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC4.0 – Criteria Related to Monitoring of Controls		
CC 4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**(Control 8)**: Management performs an annual assessment of key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements. Results are shared with senior management, tracked, and remediated in accordance with the Risk Assessment Policy.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization and that key risks were identified with potential remediating actions proposed. Inspected a sample Board of Directors meeting minutes and determined that key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements were discussed. **No deviations noted.**
	(Control 20): A third party performs penetration tests over both the network and application layers. Identified vulnerabilities rated critical or high are analyzed, tracked, and resolved according to the Vulnerability Management Program.	Inspected the Third-Party Penetration Testing Report and determined that network and application layer findings are analyzed, tracked and resolved if deemed critical or high. **No deviations noted.** Inspected evidence and determined that no critical or high findings occurred during the period of this report. **The circumstances that warrant the operation of this control step did not occur during the period of this report, as there were no critical or high vulnerabilities found during the period of this report.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**(Control 8)**: Management performs an annual assessment of key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements. Results are shared with senior management, tracked, and remediated in accordance with the Risk Assessment Policy.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization and that key risks were identified with potential remediating actions proposed. Inspected a sample Board of Directors meeting minutes and determined that key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements were discussed. **No deviations noted.**
	(Control 20): A third party performs penetration tests over both the network and application layers. Identified vulnerabilities rated critical or high are analyzed, tracked, and resolved according to the Vulnerability Management Program.	Inspected the Third-Party Penetration Testing Report and determined that network and application layer findings are analyzed, tracked and resolved if deemed critical or high. **No deviations noted.** Inspected evidence and determined that no critical or high findings occurred during the period of this report. **The circumstances that warrant the operation of this control step did not occur during the period of this report, as there were no critical or high vulnerabilities found during the period of this report.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC5.0 – Criteria Related to Control Activities		
CC 5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**(Control 8)**: Management performs an annual assessment of key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements. Results are shared with senior management, tracked, and remediated in accordance with the Risk Assessment Policy.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization and that key risks were identified with potential remediating actions proposed. Inspected a sample Board of Directors meeting minutes and determined that key internal controls relevant to the achievement of DigitalOcean's service commitments and system requirements were discussed. **No deviations noted.**
	(Control 17): DigitalOcean Security management performs an annual risk assessment to identify, evaluate, and track identified risks, including those related to fraud and the security of customer data. Based on the determined magnitude and frequency, controls are put in place to mitigate risks.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization including fraud and security and that key risks were identified with potential remediating actions proposed. **No deviations noted.**
	(Control 18): The Security team maintains a business risk matrix, which tracks identified risks, agreed-upon risk mitigation plans, and the status of risk mitigation activities.	Inspected the 2020 Business Risk tracker which identifies the key risks to the business. Additionally, inspected the 2020 Risk Register which tracks each risk, risk mitigation plans and current risk mitigation status. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 5.1 (continued)	**(Control 21)**: DigitalOcean maintains access control policies and procedures as well as documented access request procedures to enforce role-based access control (RBAC).	Inspected the Access Control Policy and Access Control Procedure, and determined that access control policies and procedures as well as documented access request procedures to enforce role-based access control (RBAC). Inspected documentation further and determined that each document was reviewed and approved annually. **No deviations noted.**
CC 5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**(Control 22)**: DigitalOcean's information security policies include requirements over the following: • The acceptable use of company assets • The use of personal devices • Protecting customer and company data • Password security and access controls	Inspected the Security policy, Acceptable Use policy, and Customer Data Use Policy, and determined that DigitalOcean's information security policies include requirements over the use of company assets, the use of personal devices, the protection of customer and company data. Inspected documentation further and determined that each document was reviewed and approved annually. **No deviations noted.**
	(Control 23): DigitalOcean maintains a Change Management Policy, which outlines the process and procedures for documenting, testing, approving, and implementing changes to the systems supporting its services.	Inspected the Change Management Policy and determined that it outlines the process and procedures for documenting, testing, approving, and implementing changes to the systems supporting its services. Inspected documentation further and determined that the policy was reviewed and approved annually. **No deviations noted.**

Criteria	**Controls specified by the Company**	**Tests Performed by EY and Results of Tests**
CC 5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**(Control 6)**: DigitalOcean maintains written policies and procedures related to Security and makes this documentation available to relevant internal employees and contractors.	Inspected policies related to Security (Information Risk Management Policy, Information Security Risk Management Procedure, Data Protection Policy, Access Control Policy and Access Control Procedure) and determined that DigitalOcean Security policies are communicated and available to employees and contractors. **No deviations noted.**
	(Control 21): DigitalOcean maintains access control policies and procedures as well as documented access request procedures to enforce role-based access control (RBAC).	Inspected the Access Control Policy and Access Control Procedure, and determined that access control policies and procedures as well as documented access request procedures to enforce role-based access control (RBAC). Inspected documentation further and determined that each document was reviewed and approved annually. **No deviations noted.**
	(Control 24): An Incident Response Policy and Plan are documented and available to employees outlining how incidents are tracked, communicated, and resolved.	Inspected the DigitalOcean Incident Response Playbook, along with other Security and Incident Response policies, and determined that the policy outlines the necessary stages of incident response for security incidents. **No deviations noted.**
CC6.0 – Criteria Related to Logical and Physical Access Controls		
CC 6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**(Control 25)**: Authentication to the DigitalOcean user-interface requires a complex password.	Inspected password policy to determine a complex password is required. Inspected password configurations to DigitalOcean user-interface and determined that DigitalOcean requires a complex password. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.1 (continued)	**(Control 26)**: New and modified user access for DigitalOcean employees requires documented approval prior to granting of access.	Inspected a listing of full-time employees hired within the period of this report and determined that employees were given baseline access to DigitalOcean applications. Inspected a sample of employees that required additional access based on their team assignment within DigitalOcean and determined that a ticket was created by the requestor and analyzed/approved by an appropriate individual prior to granting access and the access provisioned aligns with the requested access. **No deviations noted.**
	(Control 28): Logical access to systems for terminated employees is removed within one business day of their termination date.	Inspected a sample of terminated users and determined that each user's access was revoked within one business day of the user's termination date. **No deviations noted.**
	(Control 3): A formal user access provisioning process is implemented to assign or revoke access rights to contractors.	Inspected a sample of contractors that required access based on their team assignment within DigitalOcean and determined that a ticket is created by the requestor, analyzed/approved by an appropriate individual and the access provisioned aligns with the requested access. Inspected a sample of terminated contractors and determined that each contractor's access was revoked in a timely manner of the user's termination date. **No deviations noted.**

Criteria	**Controls specified by the Company**	**Tests Performed by EY and Results of Tests**
CC 6.1 (continued)	**(Control 30)**: Employee laptop authentication is configured in accordance with corporate password standards.	Inspected password policy to determine a complex password is required. Inspected employee laptop password requirements and determined that DigitalOcean requires a complex password. **No deviations noted.**
	(Control 31): The Security team uses IDS software to identify, monitor, and evaluate security threats and unusual system activity. Alerts are sent to Security personnel for items that have exceeded predefined thresholds and are tracked to resolution.	Inspected a sample of system-generated evidence showing alerts sent to the Security team and determined that DigitalOcean identifies, monitors, and evaluates security threats. Inspected a sample of tickets associated with threats and determined that threats are monitored and resolved by the Security personnel in a timely manner. **No deviations noted.**
CC 6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**(Control 26)**: New and modified user access for DigitalOcean employees requires documented approval prior to granting of access.	Inspected a listing of full-time employees hired within the period of this report and determined that employees were given baseline access to DigitalOcean applications. Inspected a sample of employees that required additional access based on their team assignment within DigitalOcean and determined that a ticket was created by the requestor and analyzed/approved by an appropriate individual prior to granting access and the access provisioned aligns with the requested access. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.2 (continued)	**(Control 28)**: Logical access to systems for terminated employees is removed within one business day of their termination date.	Inspected a sample of terminated users and determined that each user’s access was revoked within one business day of the user’s termination date. **No deviations noted.**
	(Control 32): Management performs an annual user access review to validate system access appropriateness for employee and contractor accounts.	Inspected the annual user access review conducted for in-scope system components and determined that management completed and documented review procedures. For a sample of changes recommended during the access review, determined that changes were made and procedures were performed on a timely basis. **No deviations noted.**
CC 6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.	**(Control 3)**: A formal user access provisioning process is implemented to assign or revoke access rights to contractors.	Inspected a sample of contractors that required access based on their team assignment within DigitalOcean and determined that a ticket is created by the requestor, analyzed/approved by an appropriate individual and the access provisioned aligns with the requested access. Inspected a sample of terminated contractors and determined that each contractor’s access was revoked in a timely manner of the user’s termination date. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.3 (continued)	**(Control 26)**: New and modified user access for DigitalOcean employees requires documented approval prior to granting of access.	Inspected a listing of full-time employees hired within the period of this report and determined that employees were given baseline access to DigitalOcean applications. Inspected a sample of employees that required additional access based on their team assignment within DigitalOcean and determined that a ticket was created by the requestor and analyzed/approved by an appropriate individual prior to granting access and the access provisioned aligns with the requested access. **No deviations noted.**
	(Control 32): Management performs an annual user access review to validate system access appropriateness for employee and contractor accounts.	Inspected the annual user access review conducted for in-scope system components and determined that management completed and documented review procedures. For a sample of changes recommended during the access review, determined that changes were made and procedures were performed on a timely basis. **No deviations noted.**
	(Control 33): DigitalOcean restricts access to customer data stored in production databases to designated personnel, based on documented policy.	Inspected the Access Control Policy and Access Control Procedure and determined that DigitalOcean appropriately restricts access control to corporate systems, management network systems, and the VPN that store customer data. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.3 (continued)	**(Control 34)**: The ability to deploy changes to critical infrastructure is restricted to designated personnel, in accordance with the Change Management Policy.	Inspected Change Management policies and procedures and determined that no changes can be made to critical infrastructure without a peer review and approval from another user. **No deviations noted.**
CC 6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Please refer to Section 3 – Complementary Subservice Organization Controls detailing the responsibilities of the subservice organization.	Not applicable.
CC 6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**(Control 28):** Logical access to systems for terminated employees is removed within one business day of their termination date.	Inspected a sample of terminated users and determined that each user's access was revoked within one business day of the user's termination date. **No deviations noted.**
	(Control 50): DigitalOcean has documented data backup, retention, and disposal procedures.	Inspected the Data Backup Procedure, Information Retention and Disposal Policy, and Data Backup/Replication and Retention Standard and determined employee procedures on the handling of data, data backup, data retention, and data disposal are included. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**(Control 35)**: Information in transit, including user authentication information and transmission of private or confidential information through DigitalOcean, is encrypted using Secure Sockets Layer (SSL) over Hypertext Transfer Protocol Secure (HTTPS) connections.	Inspected DigitalOcean policies that cover encryption information for data at rest and data in transit and determined that the policy and procedure information support the encryption of data across the organization. Inspected configurations and determined Information in transit, including user authentication information and transmission of private or confidential information through DigitalOcean, is encrypted using Secure Sockets Layer (SSL) over Hypertext Transfer Protocol Secure (HTTPS) connections. **No deviations noted.**
	(Control 36): DigitalOcean restricts remote access to its internal network and systems based on documented policies and through an encrypted VPN connection.	Inspected screenshots of a user attempting to gain access with and without being logged onto the VPN and determined that DigitalOcean restricts remote access to its internal network and systems through an encrypted VPN connection. **No deviations noted.**
CC 6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**(Control 35)**: Information in transit, including user authentication information and transmission of private or confidential information through DigitalOcean, is encrypted using Secure Sockets Layer (SSL) over Hypertext Transfer Protocol Secure (HTTPS) connections.	Inspected DigitalOcean policies that cover encryption information for data at rest and data in transit and determined that the policy and procedure information support the encryption of data across the organization. Inspected configurations and determined Information in transit, including user authentication information and transmission of private or confidential information through DigitalOcean, is encrypted using Secure Sockets Layer (SSL) over Hypertext Transfer Protocol Secure (HTTPS) connections. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.7 (continued)	**(Control 36)**: DigitalOcean restricts remote access to its internal network and systems based on documented policies and through an encrypted VPN connection.	Inspected screenshots of a user attempting to gain access with and without being logged onto the VPN and determined that DigitalOcean restricts remote access to its internal network and systems through an encrypted VPN connection. **No deviations noted.**
	(Control 37): IT configures employee laptops with full disk encryption.	Inspected DigitalOcean policies that cover encryption information for data at rest and data in transit and determined that policy and procedure information support the encryption of data across the organization. Inspected evidence for a sample of employee laptops and determined that laptops are configured with full disk encryption. **No deviations noted.**
CC 6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	**(Control 38)**: IT configures employee laptops with centrally managed anti-malware software to protect against threats. Software definitions are updated daily and laptops are scanned via real-time file scanning.	Inspected system-generated evidence showing employee laptop anti-malware software status and determined that devices are updated. **No deviations noted.**
	(Control 39): The Security team monitors and records potential malicious activities and behavior within DigitalOcean's production environment. Alerts are sent to Security personnel based on predefined severity.	Inspected a sample of a security incidents, including screenshots of the security alerts and associated tickets, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 6.8 (continued)	**(Control 40)**: The Infrastructure Operations team uses monitoring software to identify and evaluate ongoing system performance, average response time, error rates, and changing resource utilization needs. Alerts are sent to the Infrastructure Operations team for items that have exceeded predefined thresholds.	Inspected policies and documentation on the system performance monitoring. Through inspection determined that the Infrastructure Operations team has procedures in place to identify incidents and relay system performance to customers as needed. Inspected a sample of tickets opened and determined that customers were notified of significant issues that would potentially affect DigitalOcean products. Inspected documentation supporting the company's Capacity Planning & Management procedures which are implemented as needed based on changes in demand, availability and capacity. **No deviations noted.**
CC7.0 – Criteria Related to System Operations		
CC 7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**(Control 39)**: The Security team monitors and records potential malicious activities and behavior within DigitalOcean's production environment. Alerts are sent to Security personnel based on predefined severity.	Inspected a sample of a security incidents, including screenshots of the security alerts and associated tickets, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**(Control 39)**: The Security team monitors and records potential malicious activities and behavior within DigitalOcean's production environment. Alerts are sent to Security personnel based on predefined severity.	Inspected a sample of a security incidents, including screenshots of the security alerts and associated tickets, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**
	(Control 40): The Infrastructure Operations team uses monitoring software to identify and evaluate ongoing system performance, average response time, error rates, and changing resource utilization needs. Alerts are sent to the Infrastructure Operations team for items that have exceeded predefined thresholds.	Inspected policies and documentation on the system performance monitoring. Through inspection determined that the Infrastructure Operations team has procedures in place to identify incidents and relay system performance to customers as needed. Inspected a sample of tickets opened and determined that customers were notified of significant issues that would potentially affect DigitalOcean products. Inspected documentation supporting the company's Capacity Planning & Management procedures which are implemented as needed based on changes in demand, availability and capacity. **No deviations noted.**
CC 7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**(Control 39)**: The Security team monitors and records potential malicious activities and behavior within DigitalOcean's production environment. Alerts are sent to Security personnel based on predefined severity.	Inspected a sample of a security incidents, including screenshots of the security alerts and associated tickets, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**
	(Control 41): Incidents are tracked and resolved based on impact and risk through the ticketing system, where details of the identification, containment, remediation, and communication are maintained.	Inspected a sample of security incidents, including screenshots of the security alerts and the associated ticket, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**(Control 24)**: An Incident Response Policy and Plan are documented and available to employees outlining how incidents are tracked, communicated, and resolved.	Inspected the DigitalOcean Incident Response Playbook, along with other Security and Incident Response policies, and determined that the policy outlines the necessary stages of incident response for security incidents. **No deviations noted.**
	(Control 41): Incidents are tracked and resolved based on impact and risk through the ticketing system, where details of the identification, containment, remediation, and communication are maintained.	Inspected a sample of security incidents, including screenshots of the security alerts and the associated ticket, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**
CC 7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.	**(Control 24)**: An Incident Response Policy and Plan are documented and available to employees outlining how incidents are tracked, communicated, and resolved.	Inspected the DigitalOcean Incident Response Playbook, along with other Security and Incident Response policies, and determined that the policy outlines the necessary stages of incident response for security incidents. **No deviations noted.**
	(Control 41): Incidents are tracked and resolved based on impact and risk through the ticketing system, where details of the identification, containment, remediation, and communication are maintained.	Inspected a sample of security incidents, including screenshots of the security alerts and the associated tickets, and determined that incidents are communicated, tracked, and resolved. **No deviations noted.**
CC 8.0 – Common Criteria Related to Change Management		
CC 8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**(Control 34)**: The ability to deploy changes to critical infrastructure is restricted to designated personnel, in accordance with the Change Management Policy.	Inspected Change Management policies and procedures and determined that no changes can be made to critical infrastructure without a peer review and approval from another user. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 8.1 (continued)	**(Control 42)**: Code changes are authorized, tested, and approved prior to deployment into production, based on the size and impact of the change in accordance with the Change Management Policy.	Inspected change management policies and process and determined that significant code changes made to in-scope products are tracked through tickets. Inspected a sample of tickets that showed actionable system changes and determined that code changes/pull requests are authorized, tested, and approved prior to deployment into production. **No deviations noted.**
	(Control 47): GitHub Enterprise is the source code repository utilized across the organization. Source code changes and comments are logged in the system. Users login with unique credentials to the repository.	Inspected screenshots containing password requirements and determined that users log in with unique credentials and that users are unable to change the underlying source code repositories without approval or approved administrative access. Inquired about and inspected screenshots of GitHub Enterprise Site Admins and determined that access to implement changes without approval is restricted. **No deviations noted.**
	(Control 48): DigitalOcean utilizes the Operational Acceptance Review process to help ensure the company is prepared to operate, maintain and troubleshoot products and services once they are in production.	Inspected change management policies and process and determined that significant code changes made to in-scope products are tracked through tickets. Inspected tickets that showed actionable system changes and determined that code changes/pull requests are authorized, tested, and approved prior to deployment into production. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 8.1 (continued)	**(Control 27)**: DigitalOcean supports the segregation of duties and role-based assignment of access privileges to users within the DigitalOcean user-interface and supporting infrastructure.	Inspected the permissions for a sample of code repositories and determined that the ability to deploy changes to infrastructure is restricted to designated personnel and supports role-based assignment of access. Additionally, inspected the settings for a sample of code repositories and determined that each repository is configured to support segregation of duties. **No deviations noted.**
CC 9.0 – Common Criteria Related to Risk Mitigation		
CC 9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**(Control 17)**: DigitalOcean Security management performs an annual risk assessment to identify, evaluate, and track identified risks, including those related to fraud and the security of customer data. Based on the determined magnitude and frequency, controls are put in place to mitigate risks.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization including fraud and security and that key risks were identified with potential remediating actions proposed. **No deviations noted.**
	(Control 43): The risk management program includes the use of insurance to minimize the financial impact of cyber events.	Inquired with management and through inspection determined that DigitalOcean holds Cyber Insurance to minimize the financial impact of cyber events. **No deviations noted.**
	(Control 50): DigitalOcean has documented data backup, retention, and disposal procedures.	Inspected the Data Backup Procedure, Information Retention and Disposal Policy, and Data Backup/Replication and Retention Standard and determined employee procedures on the handling of data, data backup, data retention, and data disposal are included. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
CC 9.2 – The entity assesses and manages risks associated with vendors and business partners.	**(Control 17)**: DigitalOcean Security management performs an annual risk assessment to identify, evaluate, and track identified risks, including those related to fraud and the security of customer data. Based on the determined magnitude and frequency, controls are put in place to mitigate risks.	Inspected the 2020 Risk Assessment and determined that a variety of risk inputs were considered in order to identify key areas of risk at the organization including fraud and security and that key risks were identified with potential remediating actions proposed. **No deviations noted.**
	(Control 19): DigitalOcean management performs vendor security review procedures over third-party service providers who store or access customer data prior to engaging the third party and annually thereafter.	Inspected system-generated evidence of Vendor Security Reviews performed within the period of this report and determined security related risks of each vendor were evaluated prior to contract commencement. Inspected a sample of Vendor Security Reviews and determined that each review consisted of a security review and a legal/contract review. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
A 1.1 – Additional Criteria for Availability		
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.	**(Control 40)**: The Infrastructure Operations team uses monitoring software to identify and evaluate ongoing system performance, average response time, error rates, and changing resource utilization needs. Alerts are sent to the Infrastructure Operations team for items that have exceeded predefined thresholds.	Inspected policies and documentation on the system performance monitoring. Through inspection determined that the Infrastructure Operations team has procedures in place to identify incidents and relay system performance to customers as needed. Inspected a sample of tickets opened and determined that customers were notified of significant issues that would potentially affect DigitalOcean products. Inspected documentation supporting the company's Capacity Planning & Management procedures which are implemented as needed based on changes in demand, availability and capacity. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
A 1.2 – Additional Criteria for Availability		
The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**(Control 50)**: DigitalOcean has documented data backup, retention, and disposal procedures.	Inspected the Data Backup Procedure, Information Retention and Disposal Policy, and Data Backup/Replication and Retention Standard and determined employee procedures on the handling of data, data backup, data retention, and data disposal are included. **No deviations noted.**
	(Control 40): The Infrastructure Operations team uses monitoring software to identify and evaluate ongoing system performance, average response time, error rates, and changing resource utilization needs. Alerts are sent to the Infrastructure Operations team for items that have exceeded predefined thresholds.	Inspected policies and documentation on the system performance monitoring. Through inspection determined that the Infrastructure Operations team has procedures in place to identify incidents and relay system performance to customers as needed. Inspected a sample of tickets opened and determined that customers were notified of significant issues that would potentially affect DigitalOcean products. Inspected documentation supporting the company's Capacity Planning & Management procedures which are implemented as needed based on changes in demand, availability and capacity. **No deviations noted.**

Criteria	Controls specified by the Company	Tests Performed by EY and Results of Tests
A 1.3 – Additional Criteria for Availability		
The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**(Control 50)**: DigitalOcean has documented data backup, retention, and disposal procedures.	Inspected the Data Backup Procedure, Information Retention and Disposal Policy, and Data Backup/Replication and Retention Standard and determined employee procedures on the handling of data, data backup, data retention, and data disposal are included. **No deviations noted.**
	(Control 40): The Infrastructure Operations team uses monitoring software to identify and evaluate ongoing system performance, average response time, error rates, and changing resource utilization needs. Alerts are sent to the Infrastructure Operations team for items that have exceeded predefined thresholds.	Inspected policies and documentation on the system performance monitoring. Through inspection determined that the Infrastructure Operations team has procedures in place to identify incidents and relay system performance to customers as needed. Inspected a sample of tickets opened and determined that customers were notified of significant issues that would potentially affect DigitalOcean products. Inspected documentation supporting the company's Capacity Planning & Management procedures which are implemented as needed based on changes in demand, availability and capacity. **No deviations noted.**