# Digital Realty Trust, Inc. / Digital Realty Trust, L.P.

## SOC 2 Report

For

Data Center Services At
DUS1, DUS2, FRA1, FRA2, FRA3, FRA4, FRA5, FRA6, FRA7,
FRA8, FRA9, FRA10, FRA11, FRA12, FRA13, FRA14, FRA15, FRA16

A Type 2 Independent Service Auditor's Report on
Controls Relevant to Security and Availability

January 1, 2023, to December 31, 2023

Attestation and Compliance Services

# TABLE OF CONTENTS

# SECTION 1

## INDEPENDENT SERVICE AUDITOR'S REPORT

# INDEPENDENT SERVICE AUDITOR'S REPORT

To Digital Realty Trust, Inc. and Digital Realty Trust, L.P. (together with their respective subsidiaries, "Digital Realty" or the "service organization"):

*Scope*

We have examined Digital Realty's accompanying description of its Data Center Services system, in Section 3, throughout the period January 1, 2023, to December 31, 2023, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that Digital Realty's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability, set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

The information included in Section 5, "Other Information Provided by Digital Realty" is presented by Digital Realty management to provide additional information and is not a part of the description. Information about Digital Realty's Management's Response to Testing Exceptions, Additional Services Offered and Control Mapping have not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Digital Realty's service commitments and system requirements based on the applicable trust services criteria.

*Service Organization's Responsibilities*

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

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;

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

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

*Service Auditor's Independence and Quality Control*

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

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

*Inherent Limitations*

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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

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

*Description of Test of Controls*

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

*Opinion*

In our opinion, in all material respects,

a. the description presents Digital Realty's Data Center Services system that was designed and implemented throughout the period January 1, 2023, to December 31, 2023, in accordance with the description criteria;
b. the controls stated in the description were suitably designed throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that Digital Realty's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period; and
c. the controls stated in the description operated effectively throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that Digital Realty's service commitments and system requirements were achieved based on the applicable trust services criteria.

*Restricted Use*

This report, including the description of the tests of controls and results thereof in Section 4, is intended solely for the information and use of Digital Realty; user entities of Digital Realty's Data Center Services system during some or all of the period January 1, 2023, to December 31, 2023, business partners of Digital Realty subject to risks arising from interactions with the Data Center Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Schellman & Company, LLC

Tampa, Florida
March 19, 2024

# SECTION 2

## MANAGEMENT'S ASSERTION

# MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Digital Realty's Data Center Services system, in Section 3, throughout the period January 1, 2023, to December 31, 2023, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Data Center Services system that may be useful when assessing the risks arising from interactions with Digital Realty's system, particularly information about system controls that Digital Realty has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

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

a. the description presents Digital Realty's Data Center Services system that was designed and implemented throughout the period January 1, 2023, to December 31, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that Digital Realty's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period; and

c. the controls stated in the description operated effectively throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that Digital Realty's service commitments and system requirements would be achieved based on the applicable trust services criteria.

Please note: the term "to the best of our knowledge and belief," and similar phrases utilized herein shall mean and refer to the actual current knowledge, as of the date of this assertion, of the Senior Vice President of Global Operations.

# SECTION 3

## DESCRIPTION OF THE SYSTEM

## Overview of Operations

**Company Background**

Digital Realty provides data center, colocation, and interconnection solutions for customers across a variety of industry verticals through a portfolio of data centers located throughout North America, Europe, South America, Asia, Australia, and Africa. This description covers the Data Center Services provided by the Digital Realty data centers noted in the table within the System Boundaries section below (the "local data center"). If a customer is not served through the local data center, the portions of this description that cover the local data center will not be relevant to that customer. In addition, as discussed below, certain services provided by Digital Realty are not within the scope of this report. For that reason, it is recommended that customers confirm the data center(s) through which they are served by contacting their Digital Realty account executive.

**Types of Services Provided**

While Digital Realty provides a variety of services to its customers, this report covers only the specific services set forth below (the "Data Center Services") and excludes all other services. Although the Data Center Services are provided on a widespread basis across Digital Realty data centers, these Data Center Services may differ to some extent across data centers, solutions, and customers. If a customer receives different Data Center Services, the portions of this description that cover the Data Center Services will not be relevant to that customer. For that reason, it is recommended that customers confirm the Data Center Services they receive by contacting their Digital Realty account executive.

The term "Data Center Services" is limited to the following services provided by Digital Realty:

- Suites or cabinets
- Physical security
- Heating, ventilation, and air conditioning (HVAC)
- Fire detection and fire suppression
- Power

While Digital Realty may provide customers the following services, they are not considered "Data Center Services" for the purpose of this Report and are, accordingly, outside the scope of this Report:

- Cross-Connect (Cross-Connect, Pack, Riser Fiber, Intra-customer Connectivity, and Metro Cross-Connect)
- Digital Realty Internet Exchange (DRIX)
- Dedicated Internet Access (DIA)
- Service Exchange
- Service Fabric

These services (and any other service provided by Digital Realty outside of the five services listed in the definition of "Data Center Services") are "Out of Scope Services."

This report and description exclude services provided by (i) subsidiaries of Digital Realty; (ii) joint ventures of which Digital Realty is directly or indirectly an equity owner, unless the report states otherwise; and (iii) Out of Scope Services.

## Principal Service Commitments and System Requirements

Digital Realty implements procedures and controls to meet its objectives for Data Center Services. Those objectives are based on the service commitments that Digital Realty makes to user entities, the laws and regulations that govern the provision of Data Center Services, and the financial, operational, and compliance requirements that Digital Realty has established for the services.

*Principal Service Commitments*

Security and availability commitments to user entities are documented and communicated in customer agreements as well as in the description of the Data Center Services provided online. Digital Realty makes the following security and availability commitments to their customers:

- Make available the services to customers for the service term
- Establish, implement, and maintain commercially reasonable industry standards for physical security and protection
- Establish, implement, and maintain commercially reasonable industry standards to make the services available
- Make available the data center space 24 hours per day, 7 days a week
- Provide services in a manner that meets applicable laws and regulations

*System Requirements*

Digital Realty establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements include the following capabilities:

- Availability Monitoring: Dedicated personnel are responsible for the 24x7 monitoring and remediation of system events affecting availability. Software and other technologies are deployed to manage system availability and capacity levels against predefined thresholds.
- Infrastructure Redundancy: Redundant infrastructure is available and configured to process transactions when primary systems are unavailable.
- Physical Security Perimeter: Security perimeters are used to protect areas that contain information and information processing facilities – using walls, controlled entry doors/gates, manned reception desks, and other measures.
- Physical Entry Controls: Policies and procedures are implemented to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Temperature and Humidity Monitoring: Temperature and humidity are monitored to maintain the environment temperature and humidity in accordance with standard guidelines for datacom equipment.
- Preventative Maintenance Program: Environmental protections receive maintenance on at least an annual basis, however for assets which are subject to condition-based maintenance other maintenance frequencies may apply in accordance with the regional maintenance policy, manufacturer’s specifications, or supplier requirements as well as local regulations or electrical requirements.
- Employee Training: Employees are required to complete training upon hire and at regular intervals to understand their obligations and responsibilities to comply with the corporate and business unit commitments and the associated system requirements.

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

# Components of the System Used to Provide the Services

**System Boundaries**

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

The scope of this report includes the Data Center Services provided to Digital Realty's customers at the Digital Realty data center facilities noted in the table below.

| Digital Realty Data Center Facilities | |
|---|---|
| DUS1 | In der Steele 25-45, Dusseldorf, Germany |
| DUS2 | In der Steele 39-45, Dusseldorf, Germany |
| FRA1 | Hanauer Landstrasse 302, Frankfurt am Main, Germany |
| FRA2 | Hanauer Landstrasse 304-304a, Frankfurt am Main, Germany |
| FRA3 | Weismuellerstrasse 21-23, Frankfurt am Main, Germany |
| FRA4 | Weismuellerstrasse 19, Frankfurt am Main, Germany |
| FRA5 | Hanauer Landstrasse 308-310, Frankfurt am Main, Germany |
| FRA6 | Hanauer Landstrasse 300-300a, Frankfurt am Main, Germany |
| FRA7 | Hanauer Landstrasse 296a-298, Frankfurt am Main, Germany |
| FRA8 | Weismuellerstrasse 36, Frankfurt am Main, Germany |
| FRA9 | Weismuellerstrasse 25-27, Frankfurt am Main, Germany |
| FRA10 | Weismuellerstrasse 38, Frankfurt am Main, Germany |
| FRA11 | Weismuellerstrasse 40, Frankfurt am Main, Germany |
| FRA12 | Weissmullerstrasse 29-31, Frankfurt am Main, Germany |
| FRA13 | Weismuellerstrasse 42, Frankfurt am Main, Germany |
| FRA14 | Weismuellerstrasse 34, Frankfurt am Main, Germany |
| FRA15 | Weismuellerstrasse 1, Frankfurt am Main, Germany |
| FRA16 | Weismuellerstrasse 37-39, Frankfurt am Main, Germany |

**Infrastructure and Software**

The infrastructure supporting the Data Center Services includes the data center building, the suites within, security cameras, physical access control devices, interconnection routers, and switches and the servers supporting the applications noted below. The building is also equipped with uninterruptible power supply (UPS), fire detection, and suppression systems, back-up generators, and HVAC systems to protect against threats to environmental security.

The primary in-scope systems utilized for delivery of the Data Center Services are the physical access control system applications and the logical access to interconnection routers and switches. These commercial badge access applications are based on the Windows operating systems, and are used to provision, de-provision, and manage user access to the building and suites contained within. Network device login and access is governed by an access control system tied to directory services. These devices serve as interconnection devices that provide

data forwarding between internal networks and Ethernet exchanges. The routers and switches include Cisco, Juniper, and Dell equipment.
Secondary applications utilized to support delivery of the Data Center Services include:

- Digital Realty DMZ application – utilized for provisioning individual IDs for third party team members to access InSite/ServiceNow.
- Building Management System (BMS) – utilized by the site engineering team to monitor and control environmental systems.
- Network Monitoring Application – utilized to detect and log changes made to network device configurations.
- Salesforce – utilized to track network changes, cross-connects, and complex installations through completion.
- ServiceNow / Insite – the third-party cloud-based Integrated Work Order Management System is utilized for Maintenance Management, Security Access & Authorization, Incident Reporting, & Customer Request modules.

The Data Center Services system is limited to the data center services and related infrastructure maintained by Digital Realty and does not include customer entity systems, or the Internet connectivity utilized for accessing their environments.

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

| **Production Systems** | | | |
|---|---|---|---|
| **Production System** | **Business Function Description** | **Operating System Platform** | **Physical Location** |
| Web, Application, and Database Servers | Application and database servers that support physical access systems. | Windows | Digital Realty property-level locations |
| Database | Physical access system data storage. | | |
| Directory Services | Provides access control and directory services for users and systems. | | |
| Commercial Badge Access Applications | Security management system supporting badge access. | | |
| Firewall and Router Systems | Front-end firewalls protect the network perimeter based on rule-based access control lists. | Juniper<br>Cisco | |
| Access Control System | Manages authentication for virtual private network (VPN), firewalls, and network devices. | Linux | |

**People**

The Chief Commercial Operations Officer leads Global Operations by implementing a global model centered around key service areas to enhance service-delivery consistency globally. The Global Operations team drives and reinforces a customer-centric, consistent approach to how Digital Realty builds and operates globally. This includes partnering with and empowering local leaders and colleagues with simplified work planning and allocation, a standard set of KPIs, and enhanced role clarity. Digital Realty's Senior Vice President (SVP) of Global Operations defines the Global Operations structure driving the global operations strategy, aligning best practice standards, and supporting regional teams to ensure global consistency for customers.

Each local entity has a dedicated local management team, responsible for data center operations in their respective region, reporting to their respective managing directors. The local Operations managers / directors have a functional reporting line to the regional Operations leadership. The local regional Operations manager / director oversees the electrical and mechanical engineering specialists who maintain and monitor platforms of the data center facilities. More specifically, the local regional Operations manager / director ensures that the specialists are properly trained, and that systems and processes are in place to ensure continual facilities uptime, system-wide security consciousness, and consistent service execution.

Digital Realty employs regional vice presidents, directors, and managers of technical operations who are responsible for process, quality, and compliance with aspects of technical operations and engineering functions. These individuals have significant experience with the operation and maintenance of diverse mission critical electrical and mechanical equipment. Core groups supporting day-to-day operations include the following:

- Facility Management / Site Engineering – responsible for operation and maintenance of diverse mission critical electrical and mechanical equipment.
- Security – responsible for 24x7 monitoring of the building, administration of physical access systems, and responding to alerts/events.
- Site Management – responsible for day to day operations of the site: operations, maintenance, physical security, billing, lease and financial reporting functions.
- Command Centers - in addition to being the single point of contact for customers, the Command Centers provide remote monitoring on critical alarms linked to assets, as configured in the local BMS. The Command Centers act as a gatekeeper for the local entities providing Incident Management coordination, corporate escalation, and emergency response communications.
- Global Customer Care – responsible for carrying out customer remote hands requests and customer services teams can manage or help support customer onboarding process and facilitate hand-off from Sales to Internal / External Construction teams as well as Operating teams who are responsible for supporting customers locally.
- Provisioning / Service Planning – documents customer orders for new cross-connects and maintains the cross-connects inventory.

**Procedures**

Procedures supporting the Data Center Services include:

*Physical Security*

Digital Realty's physical security policies are set forth in the GRC document management system which is distributed to the site management and Security teams at the local data center facilities. Physical security of the building is controlled through limited access points, and physical security of each suite is controlled through a badge and/or biometric reader. Access to master keys is restricted to emergency use only and to personnel from the Security, Engineering, and Site Management teams. New security personnel are required to undergo orientation training and existing security personnel are required to complete annual refresher training course(s).

*Visitor Procedures*

Visitors are required to check-in with the Security team and must provide valid government-issued photo ID to verify their identity. Visitors must sign in and provide the name of the Digital Realty / customer individual they will be meeting with. Temporary visitor access will be pre-authorized by the designated Digital Realty or customer host. Escort only visitors will be provided escorted access by an authorized customer or Digital Realty representative. Authorized employees and customer personnel are issued a permanent badge. Digital Realty personnel other than authorized employees and strategic partners are granted a temporary badge.

*Monitoring*

Security personnel monitor both the interior and exterior of the building through closed-circuit TV (CCTV). The data center is under 24-hour recorded CCTV camera surveillance. Cameras are also deployed within the suites and surrounding areas to monitor the security of exits and entrances. The recordings are retained for a minimum of 90 days and may be used for investigative purposes, or as otherwise legally permitted.

Security personnel also monitor card activity for access points to the building and the suites. In the event of any suspicious activity (e.g., a card reader bypass by a master key, a door being held open for an extended time, etc.), the security system initiates an alert and displays the logged event. Security personnel investigate the alert and once the issue is resolved, they record the outcome in the physical security access system.

*Security Incident Response*

Security personnel respond to security incidents and involve the appropriate resources (e.g., Digital Realty management, fire department, police, etc.) to achieve resolution. The security incidents are documented, and significant security events are reported and escalated to the Digital Realty regional Security management and are also communicated to impacted employees or customers.

*Disaster Recovery*

Digital Realty has in place disaster recovery plans for the Data Center Services that address the following:

- Risk identification, evaluation, and scoring
- Personnel assignments and team organization
- Incident response plans
- Contact information for customers, vendors, employees, emergency responders, and recovery partners
- Recovery team's tasks and procedures

Each of the above elements is tested regularly through live exercises of systems and personnel in the course of normal operations. This testing takes the following forms:

- Load testing of UPS and generator systems
- Activation of incident response communications systems to communicate with customers, vendors, employees, emergency responders, and response teams
- Activation of response teams to evaluate and respond to potentially threatening conditions
- Redundant physical access systems and environmental systems infrastructure exercises, including power and cooling systems

In each case noted above, management plans, communications, staff responses and system redundancies are validated to confirm that all perform properly to prevent or mitigate the impact on the data center operations.

Because situations in which Digital Realty has access to customer data are very limited generally and even more so with the defined Services system, back-up procedures for customer data are considered outside the boundaries of this system and are the user entities' responsibilities.

*Customer Contact List*

For every customer, Digital Realty maintains a list of customer personnel (the "customer contact list") that can approve user account requests. Customer access is self-managed by the customer via the Customer Portal for real time updates for the site management and security teams.

*User Access Requests and Provisioning*

Security personnel will issue badges or grant access (I) to a customer's employees or contractors based on documented approvals obtained from an authorized approver identified in the corresponding customer contact list and (ii) to Digital Realty's employees or contractors based on approvals obtained from Digital Realty's Site Management or Site Engineering team.

*User Access Revocation*

An individual's access to the building is disabled through the physical security access system upon request by the authorized customer or Digital Realty personnel. Upon the termination of any Digital Realty employee or contractor, HR sends a notification via the ticketing system that is routed to the physical security access system administrators to disable the employee/contractor access. A confirmation e-mail is sent upon removal and tracked in the ticketing system.

*Internal Security Assessment Program*

The Portfolio Security Team performs an internal security assessment program annually as part of the "Digital Realty Center of Operational Excellence Program." As part of this quality assurance program, internal auditors evaluate the current security operating procedures and address any areas which are inconsistent with standard operating procedures.

*Environmental Controls*

Environmental controls are maintained by the Facility Management/Site Engineering team. The Site Engineering team for each data center consists of a property Facility Manager/Chief Engineer and building engineers. The team reports to the Data Center Manager. The Site Engineering team uses an online BMS to monitor and control the environmental systems that support the building and the suites. The Facility Management/Site Engineering team tracks alerts through to resolution.

*Uninterruptible Power Supply (UPS / Batteries)*

UPS systems are in place to ensure uninterrupted power supply in case of a power outage. The current operational state of the UPS systems is monitored by site personnel. Preventative maintenance is performed at least annually.

*HVAC Systems*

The HVAC systems control and monitor temperature and humidity levels within the building and the suites. The chilling loop system has a cooling capacity greater than the required cooling capacity. The units are monitored and any change in temperature or humidity levels outside of a pre-set threshold triggers an alert that is sent to the Site Engineering team for resolution. Preventative maintenance is performed at least annually.

*Fire Suppression; Fire and Smoke Detection*

Fire and smoke detectors and fire extinguishers are present throughout the building and the suites. The fire suppression systems are either automatic gas-based fire suppression systems or double interlock pre-action systems. The double interlock pre-action systems require two triggers – a fusible link melting and a signal from the pre-action detection system. Unless both of these triggers are initiated, water does not enter the water mist fire suppression or sprinkler piping system. Preventative maintenance is performed at least annually.

*Generators*

Generators are in place to support the base building and the suites in an event of a prolonged power failure. The current operational state of each of the generators is monitored by site personnel. Preventative maintenance is performed at least annually.

**Data**

The data relevant to the in-scope systems include user account information, access lists, and physical and environmental event logs and reports. User account information is submitted through the online customer service system and the request (provisioning/de-provisioning) is executed in the physical security access system. Access to this data is limited to authorized personnel through logical access controls for the in-scope systems and considered as classified information by Digital Realty personnel.

Because situations in which Digital Realty has access to customer data are very limited generally and even more so with the defined Services system, customer data, including data maintained on back-up media or servers, is not included in the scope of this assessment.

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

<table>
<tr><th colspan="3">Data Used and Supported by the System</th></tr>
<tr><th>Data Description</th><th>Data Reporting</th><th>Classification</th></tr>
<tr><td>Physical security data that include access logs and video surveillance images.</td><td rowspan="3">This data is not reported to customers unless required for investigative purposes.</td><td rowspan="2">Classified</td></tr>
<tr><td>Environmental security monitoring log data regarding the status of the environmental monitoring systems.</td></tr>
<tr><td>Environmental security data that include inspection reports for fire detection, fire suppression, water intrusion, cooling systems, power equipment (UPS, generator, etc.), humidity, etc.</td><td>Restricted</td></tr>
</table>

### Significant Changes During the Period

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

### Subservice Organizations

No subservice organizations were relevant to the scope of this assessment whose controls were necessary, in combination with controls at Digital Realty, to provide reasonable assurance that Digital Realty's service commitments and system requirements were achieved.

## CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors (BoD) and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the BoD to carry out its oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

### Commitment to Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Digital Realty's control environment, affecting the design, administration, and monitoring of other components.

Integrity and ethical behavior are the products of Digital Realty's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of ethical values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that Digital Realty has implemented in this area are described below.

- A documented code of conduct is in place to govern workplace behavior standards.
- Management formally documents and reviews organizational updates that communicate entity values and behavioral standards to personnel on an annual basis.
- Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures.
- Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet.
- Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
- Background checks are performed for employees as a component of the hiring process, to the extent permissible by local law.

**Board Oversight Responsibility**

Digital Realty's control consciousness is influenced by its BoD and audit committee. Attributes that contribute toward this influence include the collective professional experience of the BoD, involvement in, and scrutiny of, company activities, performing its fiduciary duties, and interaction with the company's internal and external auditors as well as the degree to which difficult questions are raised and pursued with management. The BoD consists of eleven directors, including a chairman, who participate in regularly scheduled meetings to ensure key information is received in a timely manner. Except for the President & Chief Executive Officer (CEO), all members of the BoD are independent. The audit committee meets on a regular basis with management and the internal and external auditors to discuss the financial reporting process, system of internal controls, significant comments and recommendations, and management's performance. Specific control activities that Digital Realty has implemented in this area are described below.

- BoD governance documents are in place that outline board member responsibilities, mandates, including for management oversight, and oversight of internal control.
- Performance plans are approved by the Compensation Committee to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against.
- The BoD has sufficient members who are independent from management and are objective in evaluations and decision making.
- The BoD meets on an annual basis to review and approve strategic company objectives and the performance of internal control.

**Structure, Authority, and Responsibility**

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

Digital Realty's assignment of authority and responsibility includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how, and for what, they will be held accountable. Specific control activities that Digital Realty has implemented in this area are described below.

- Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.
- The organizational charts are available and communicated to employees and updated as needed.
- Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
- Management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team.

**Commitment to Competence**

Digital Realty management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Digital Realty's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Training of personnel is conducted through supervised on-the-job training, externally offered seminars, and in-house courses. Specific control activities that Digital Realty has implemented is this area are described below.

- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
- Operations employees are required to complete security awareness training, upon hire, and annually, to understand their obligations, and responsibilities to comply with the corporate and business unit security policies.
- Management monitors compliance with training requirements on an annual basis.
- Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
- Employee acknowledgments are conducted by management personnel on an annual basis to help ensure employee compliance with the code of conduct.

**Accountability**

Digital Realty management's philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. Digital Realty's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Digital Realty has implemented in this area are described below.

- Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
- Management provides internal control performance metrics and third-party audit results to the BoD on an annual basis.
- Employee acknowledgments are conducted by management personnel on an annual basis to help ensure employee compliance with the code of conduct.
- Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.

# RISK ASSESSMENT

### Objective Setting

The risk assessment process involves a dynamic process that includes the identification and analysis of risks that pose a threat to the organization's ability to perform the services. The process first starts with determining the organization's objectives as these objectives are key to understanding the risks and allows the identification and analysis of those risks relative to the objectives. Management has committed to customers to carry out certain objectives in relation to the services provided. These commitments are documented and reviewed as part of customer contracts and specific service level agreements (SLAs) to ensure that the operations, reporting, and compliance objectives are aligned with the commitments and company's mission.

### Risk Identification and Analysis

Digital Realty has established processes to identify and manage risks that could affect the organization's ability to provide reliable services for user entities. Based on the defined scope of the Services, the primary risk categories include risk of critical building system failure and risk of physical security compromise. Digital Realty employs a Vice President of Risk Management to support risk assessment and response.

The risk of critical building system failure has a non-customer specific component which is systemic and a customer specific component that is slightly different for each customer. The non-customer specific component relates to the proper maintenance, monitoring and operations of the core infrastructure building systems, including the normal, emergency, and uninterruptible power supply and the central cooling plants. Risks to these systems are assessed initially via third party commissioning activities and regularly thereafter by way of multi-tiered proactive monitoring activities. Customer specific risks typically relate to the proper loading of electrical panels and the proper hardware footprint with respect to cooling tolerances. These risks are assessed initially by the customer and Digital Realty's Sales Engineering team during the design of each customer's interior space and monitoring/maintenance activity is planned accordingly.

Physical security risks consist primarily of risks associated with access violation and hardware / software misuse. These risks are assessed upon initial design of the space. Digital Realty's Physical Security team continually assesses local or time-specific risks and customers are advised to periodically update and review access authorization rights.

On at least an annual basis, risks are assessed to identify threats to the achievement of the security and availability objectives and commitments. Identified risks and threats are documented and the risks are rated along with mitigation strategies. Based on these ratings, a table-top exercise is performed at each data center facility or campus on an annual basis. As part of the annual exercise, property team members complete an online training course, and each site or campus team then conducts the table-top exercise for the specific threat.

In addition, Digital Realty holds change management meetings on at least a monthly basis, at which upcoming maintenance or other events that could impact the building systems or security environment are detailed. Customers are asked for input and event scheduling is adjusted to suit timing sensitivities. Significant issues are elevated to senior management as appropriate.

### Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

*External Factors*

- Technological developments and incidents
- Changing customer needs or expectations
- Competition that could alter marketing or service activities

- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

*Internal Factors*

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

**Potential for Fraud**

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws. Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. The annual enterprise-wide risk assessment process considers the potential for fraud.

**Risk Mitigation**

Risk remediation is the process for managing project activities or circumstances that may result in negative consequences to Digital Realty. Risk mitigation activities are activities that will remediate the risk to an acceptable level (agreed upon by the Data Center Manager and Risk Owner). Timeline, point of contact, and action plan are required to be documented as part of the risk mitigation strategy.

## TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

**Integration with Risk Assessment**

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

**Selection and Development of Control Activities**

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

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

**Trust Services Criteria Not Applicable to the In-Scope System**

The Trust Services criteria presented below, are not applicable to the Data Center Services system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criteria.

The following table presents the trust services criteria that are not applicable for the Data Center Services system at Digital Realty. The not applicable trust services criteria are also described within Section 4.

| Criteria # | Reason for Omitted Criteria |
|---|---|
| CC6.6<br>CC6.7 | The Digital Realty in-scope systems do not transmit, move, or remove data outside the boundaries of the system and Digital Realty does not administer logical access to systems for user entities. |

## INFORMATION AND COMMUNICATION SYSTEMS

Digital Realty has integrated operations systems and monitoring and detection systems, such as the BMS, that allow pertinent information to be identified, captured, and communicated, in sufficient detail, and in a timeframe, that allows employees to carry out their responsibilities. Digital Realty's information systems provide information to help identify risks and opportunities, and high-quality information to manage and control activities. Information systems are relied upon for the achievement of company-level and process / application-level objectives.

Digital Realty has implemented information systems to help ensure that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation and training for new employees and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate with their supervisor or executive management.

Digital Realty has implemented various methods of communication to ensure that employees understand their individual roles and responsibilities related to processes and controls, and to help ensure that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees, a web-based knowledge base with detailed policies, and the use of e-mail messages to communicate time-sensitive messages and information. Managers also hold periodic staff meetings as appropriate. Employees are responsible for communicating significant issues and exceptions to an appropriate higher level of authority within the organization in a timely manner.

Personnel in Digital Realty's Customer Services team provide ongoing communication with customers. The Customer Services team maintains records of incidents reported by customers and incidents noted during processing and monitor such items until they are resolved. The Customer Services team supports the Site Management team and communicates information regarding changes in processing schedules, system enhancements, and other information to customers.

Internally, service requests associated with normal, or emergency maintenance activities are distributed electronically to Digital Realty technicians' computers and/or handheld devices. Key Digital Realty personnel attend monthly operations management meetings to discuss ongoing and upcoming activities. These activities are communicated to customers at the facility who are invited to provide feedback on dates, timeframes, and related matters regarding the activities.

Digital Realty's Onboarding Process details protocols for communication with respect to critical technical issues and security, including escalation protocols. Each Digital Realty customer is provided a single point of contact at Digital Realty and Digital Realty works with each customer prior to occupancy to derive a custom reporting package based on variables that such customer deems relevant, which can include maintenance reports, alarm indications, access events and key power / cooling-related performance indicators.

# MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluations, or a combination of the two. Monitoring activities also include using information from communications from external parties, such as user entity complaints and regulatory comments, that may indicate problems, or highlight areas in need of improvement.

*Ongoing Monitoring*

Digital Realty uses multiple methods to proactively monitor critical building systems related to physical security and environmental controls. With respect to security and access control, Digital Realty's Security personnel monitor closed-circuit television feeds from cameras throughout the interior and exterior of the site, perform daily rounds within the building and site, and log, and monitor access events via an access control software platform. Staff continually monitors the building's entrances and oversees shipping / receiving and visitor activity, as necessary. With respect to environmental controls, the Site Engineering team monitors the BMS in addition to receiving and responding to alerts for any variations outside of the pre-set thresholds. An intrusion detection system (IDS) is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification.

*Internal and External Auditing*

Digital Realty maintains an independent, objective, and professionally staffed internal audit function. Internal audit's main mission, in direct support of management, the BoD, and the audit committee, is to provide assurance as to the adequacy and effectiveness of the overall internal control environment. Internal audit shares best practices, makes recommendations, and proposes ideas designed to further improve the service organization's overall control environment, thereby delivering cost savings, revenue enhancements, and process improvements. The internal audit team is authorized to have unrestricted access to functions, records, property, and personnel and has full and free access to the audit committee. Internal audit is responsible for conducting audits and reviews of Digital Realty's operational, financial, and IT internal control environment. These may encompass a single function or activity, a department, or an entire division.

Internal audit reports its findings and makes recommendations to managers who are responsible for implementing them. Reports are also distributed to relevant members of senior management, the chair of the audit committee, and external auditors, as appropriate. Internal audit meets with the audit committee and with senior management during the year to report on plans, activities, findings, and concerns. Internal audit also monitors management's progress towards completion of required remediation.

Digital Realty supports user entities in their efforts to meet the regulatory demands of their industry or governing agency and has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands.

**Evaluating and Communicating Deficiencies**

Identified performance deficiencies reported by a customer, third party assessments, or the service organization's monitoring activities will be logged into an incident management system for investigation and resolution. Customer complaints and comments are logged and reviewed to identify improvements in daily operations at each data center location.

# COMPLEMENTARY CONTROLS AT USER ENTITIES

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

# SECTION 4

## TESTING MATRICES

# TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

**Scope of Testing**

This report on the controls relates to the Data Center Services system provided by Digital Realty. The scope of the testing was restricted to the Data Center Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period January 1, 2023, through December 31, 2023.

Control activities that are denoted as “Centralized” are processes that are either managed at the entity level or regionally.

Control activities that are denoted as “Site Level” are processes that are directly managed by site management teams.

**Tests of Operating Effectiveness**

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

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

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

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

<u>Sampling</u>

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

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

### Reliability of Information Provided by the Service Organization

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

### Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

## SECURITY CATEGORY

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **Control Environment** | | | |
| **CC1.1** COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | | |
| CC1.1.1 **Centralized** | A documented code of conduct is in place to govern workplace behavior standards. | Inspected the code of conduct to determine that a documented code of conduct was in place to govern workplace behavior standards. | No exceptions noted. |
| CC1.1.2 **Centralized** | Management formally documents and reviews organizational updates that communicate entity values and behavioral standards to personnel on an annual basis. | Inspected the corporate security policies and procedures to determine that management formally documented and reviewed organizational updates that communicated entity values and behavioral standards to personnel during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC1.1.3 **Centralized** | Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. | Inspected the signed acknowledgments for a sample of employees hired during the period to determine that each employee sampled signed an acknowledgement form upon hire indicating that they had been given access to the employee policies and procedures and understood their responsibility for adhering to the code of conduct outlined within the policies and procedures. | No exceptions noted. |
| CC1.1.4 **Centralized** | Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. | Inspected the security policies and customer handbook displayed on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements were communicated to internal personnel via the company Intranet. | No exceptions noted. |
| CC1.1.5 **Centralized** | Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. | Inspected the code of conduct to determine that policies were documented and maintained that address remedial actions for lack of compliance with policies and procedures. | No exceptions noted. |
| CC1.1.6 **Centralized** | Background checks are performed for employees as a component of the hiring process, to the extent permissible by local law. | Inspected the completed background check documentation for a sample of employees hired during the period to determine that background checks were performed as a component of the hiring process to the extent permissible by local law for each employee sampled. | No exceptions noted. |
| **CC1.2** COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | | |
| CC1.2.1 **Centralized** | BoD governance documents are in place that outline board member responsibilities, mandates, including for management oversight, and oversight of internal control. | Inspected the BoD governance guidelines and committee charters to determine that BoD governance documents were in place that outlined board member responsibilities, mandates, including for management oversight, and oversight of internal control. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC1.2.2 **Centralized** | Performance plans are approved by the Compensation Committee to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against. | Inspected the BoD committee meeting agenda to determine that performance plans were approved by the Compensation Committee to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against. | No exceptions noted. |
| CC1.2.3 **Centralized** | The BoD has sufficient members who are independent from management and are objective in evaluations and decision making. | Inspected the BoD personnel listing and organizational chart to determine that the BoD had sufficient members who were independent from management and were objective in evaluations and decision making. | No exceptions noted. |
| CC1.2.4 **Centralized** | The BoD meets on an annual basis to review and approve strategic company objectives and the performance of internal control. | Inspected the BoD committee meeting minutes to determine that the BoD met on an annual basis to review and approve strategic company objectives and the performance of internal control. | No exceptions noted. |
| **CC1.3** COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| CC1.3.1 **Centralized** | Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. | Inspected the company organizational chart to determine that an organizational chart was in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and updated as needed. | No exceptions noted. |
| CC1.3.2 **Centralized** | Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | Inspected documented position descriptions for a sample of actively used job descriptions to determine that documented position descriptions were in place for employment positions to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | No exceptions noted. |
| CC1.3.3 **Centralized** | Management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team. | Inspected the company organizational chart and information security policies to determine that management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC1.4** COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| CC1.4.1 **Centralized** | New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description. | Inspected the employee hiring procedures to determine that new employee hiring procedures included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description. | No exceptions noted. |
| CC1.4.2 **Centralized** | Training courses are available to new and existing employees to maintain and advance the skill level of personnel. | Inspected the digital university training portal to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel. | No exceptions noted. |
| CC1.4.3 **Centralized** | Operations employees are required to complete security awareness training, upon hire, and annually, to understand their obligations, and responsibilities to comply with the corporate and business unit security policies. | Inspected the security training documentation for a sample of current operations employees and operations employees hired during the period to determine that each employee sampled completed security awareness training upon hire and during the period to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | No exceptions noted. |
| CC1.4.4 **Centralized** | Management monitors compliance with training requirements on an annual basis. | Inspected the security training monitoring documentation to determine that management monitored compliance with training requirements during the period. | No exceptions noted. |
| CC1.4.5 **Centralized** | Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | Inspected documented position descriptions for a sample of actively used job descriptions to determine that documented position descriptions were in place for employment positions to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC1.4.6 **Centralized** | Employee acknowledgments are conducted by management personnel on an annual basis to help ensure employee compliance with the code of conduct. | Inspected the signed acknowledgments for a sample of current employees during the period to determine that the sampled employees and contractors signed an acknowledgement form at least annually, indicating that they had been given access to the employee policies and procedures and understood their responsibility for adhering to the code of conduct outlined within the policies and procedures. | No exceptions noted. |
| **CC1.5** COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | | |
| CC1.5.1 **Centralized** | Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | Inspected documented position descriptions for a sample of actively used job descriptions to determine that documented position descriptions were in place for employment positions to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | No exceptions noted. |
| CC1.5.2 **Centralized** | Management provides internal control performance metrics and third-party audit results to the BoD on an annual basis. | Inspected the BoD committee meeting minutes to determine that management provided internal control performance metrics and third-party audit results to the BoD during the period. | No exceptions noted. |
| CC1.5.3 **Centralized** | Employee acknowledgments are conducted by management personnel on an annual basis to help ensure employee compliance with the code of conduct. | Inspected the signed acknowledgments for a sample of current employees during the period to determine that the sampled employees and contractors signed an acknowledgement form at least annually, indicating that they had been given access to the employee policies and procedures and understood their responsibility for adhering to the code of conduct outlined within the policies and procedures. | No exceptions noted. |
| CC1.5.4 **Centralized** | Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. | Inspected the code of conduct to determine that policies were documented and maintained that address remedial actions for lack of compliance with policies and procedures. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **Communication and Information** | | | |
| **CC2.1** COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | | |
| CC2.1.1 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| CC2.1.2 **Centralized** | A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities.  Findings are remediated according to internal policy SLAs. | Inspected the threat and vulnerability management policy and a sample of closed tickets from the ticketing system during the period to determine that a formal threat and vulnerability management process was in place for addressing identified threats and vulnerabilities and findings were remediated according to internal policy SLAs for each ticket sampled. | No exceptions noted. |
| CC2.1.3 **Site Level** | Security management systems are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. | Observed the security management system at each data center facility to determine that security monitoring applications were utilized to monitor and analyze the in-scope systems for possible or actual security breaches. | No exceptions noted. |
| CC2.1.4 **Site Level** | Security staff continuously monitors the security management system in real-time that captures card activity of access points to the Building and access points to the Suites. Security staff acknowledge the logged exception events to evidence resolution. | Observed security staff personnel at each data center and inspected the badge access history logs to determine that security staff monitored the security management system in real-time that captured card activity of access points to the facility and access points to the customer suites and acknowledged the logged exception events to evidence resolution. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC2.1.5 **Centralized** | Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. | Inspected the security policies and customer handbook displayed on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements were communicated to internal personnel via the company Intranet. | No exceptions noted. |
| CC2.1.6 **Centralized** | Annual assessments are performed by the compliance team. These assessments include evaluation of the operation of key controls. Assessments are reviewed and require the development of corrective action plans for control weaknesses. | Inspected the most recently completed security standardized assessments for a sample of data center facilities performed during the period to determine that annual assessments were performed by the compliance team, and these assessments included evaluation of the operation of key controls, assessments were reviewed, and required the development of corrective action plans for control weaknesses for each facility sampled. | No exceptions noted. |
| CC2.1.7 **Centralized** | The IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. | Inspected an example security update e-mail notification during the period to determine that the IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management. | No exceptions noted. |
| **CC2.2** COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | | |
| CC2.2.1 **Centralized** | Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. | Inspected the security policies and customer handbook displayed on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements were communicated to internal personnel via the company Intranet. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC2.2.2 **Centralized** | Operations employees are required to complete security awareness training, upon hire, and annually, to understand their obligations, and responsibilities to comply with the corporate and business unit security policies. | Inspected the security training documentation for a sample of current operations employees and operations employees hired during the period to determine that each employee sampled completed security awareness training upon hire and during the period to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | No exceptions noted. |
| CC2.2.3 **Centralized** | Management monitors compliance with training requirements on an annual basis. | Inspected the security training monitoring documentation to determine that management monitored compliance with training requirements during the period. | No exceptions noted. |
| CC2.2.4 **Centralized** | Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | Inspected documented position descriptions for a sample of actively used job descriptions to determine that documented position descriptions were in place for employment positions to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. | No exceptions noted. |
| CC2.2.5 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC2.2.6 **Centralized** | Annual assessments are performed by the compliance team. These assessments include evaluation of the operation of key controls. Assessments are reviewed and require the development of corrective action plans for control weaknesses. | Inspected the most recently completed standardized assessments for a sample of data center facilities performed during the period to determine that annual assessments were performed by the compliance team, and these assessments included evaluation of the operation of key controls, assessments were reviewed, and required the development of corrective action plans for control weaknesses for each facility sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC2.2.7 **Centralized** | The compliance team sends a monthly internal notification to communicate planned changes to the organization. | Inspected the monthly onsite newsletter for a sample of months to determine that the compliance team sent a monthly internal notification to communicate planned changes to the organization for each month sampled. | No exceptions noted. |
| CC2.2.8 **Centralized** | Management holds an annual company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives. | Inspected the company-wide strategy meeting to determine that management held an annual company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives. | No exceptions noted. |
| **CC2.3** COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| CC2.3.1 **Centralized** | The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. | Inspected the customer contracts for a sample of new customers during the period to determine that the entity's security and availability commitments and the associated system requirements were documented in customer agreements to include relevant service level and nondisclosure terms for each customer sampled. | No exceptions noted. |
| CC2.3.2 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC2.3.3 **Centralized** | Annual assessments are performed by the compliance team. These assessments include evaluation of the operation of key controls. Assessments are reviewed and require the development of corrective action plans for control weaknesses. | Inspected the most recently completed security standardized assessments for a sample of data center facilities performed during the period to determine that annual assessments were performed by the compliance team, and these assessments included evaluation of the operation of key controls, assessments were reviewed, and required the development of corrective action plans for control weaknesses for each facility sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC2.3.4 **Centralized** | The entity's security and availability commitments and the associated system requirements are documented in vendor contracts and nondisclosure agreements for critical vendors. | Inspected the vendor contracts and nondisclosure agreements for a sample of critical vendors during the period to determine that the entity's security and availability commitments and the associated system requirements were documented in critical vendor contracts and nondisclosure agreements for each vendor sampled. | No exceptions noted. |
| CC2.3.5 **Site Level** | The director of site operations performs an annual review of the Digital Realty security post orders including system security changes that might impact local property teams. The approved post orders are disseminated to the local site management by site operations. | Inspected the Digital Realty security post orders to determine that the director of site operations performed an annual review of the Digital Realty security post orders including system security changes that might impact local property teams. The approved post orders are disseminated to the local site management by site operations. | No exceptions noted. |
| **Risk Assessment** | | | |
| **CC3.1** COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| CC3.1.1 **Centralized** | Management holds an annual company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives. | Inspected the company-wide strategy meeting to determine that management held an annual company-wide strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives. | No exceptions noted. |
| CC3.1.2 **Centralized** | Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC3.1.3 **Centralized** | Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the property risk assessment completed during the period for a sample of data center facilities to determine that technical operations performed a risk assessment during the period to identify and analyze the business and security risks, vulnerabilities, laws, and regulations, and the risk assessment also included the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system and risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies for each data center facility sampled. | No exceptions noted. |
| **CC3.2** COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | | | |
| CC3.2.1 **Centralized** | Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC3.2.2 **Centralized** | Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the property risk assessment completed during the period for a sample of data center facilities to determine that technical operations performed a risk assessment during the period to identify and analyze the business and security risks, vulnerabilities, laws, and regulations, and the risk assessment also included the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system and risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies for each data center facility sampled. | No exceptions noted. |
| CC3.2.3 **Site Level** | Security staff continuously monitors the security management system in real-time that captures card activity of access points to the Building and access points to the Suites. Security staff acknowledge the logged exception events to evidence resolution. | Observed security staff personnel at each data center and inspected the badge access history logs to determine that security staff monitored the security management system in real-time that captured card activity of access points to the facility and access points to the customer suites and acknowledged the logged exception events to evidence resolution. | No exceptions noted. |
| CC3.2.4 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| **CC3.3** COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | | |
| CC3.3.1 **Centralized** | Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. | Inspected the risk assessment policy to determine that policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC3.3.2 **Centralized** | A risk assessment is performed on an annual basis that considers the potential for fraud. Identified risks are rated using a risk evaluation process and are formally documented for management review. | Inspected a sample of property risk assessments completed during the period to determine that a risk assessment was performed that considered the potential for fraud and that identified risks were rated using a risk evaluation process and were formally documented for management review during the period. | No exceptions noted. |
| **CC3.4** COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| CC3.4.1 **Centralized** | The IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. | Inspected an example security update e-mail notification received during the period to determine that the IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management. | No exceptions noted. |
| CC3.4.2 **Centralized** | Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | No exceptions noted. |
| CC3.4.3 **Centralized** | Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. | Inspected the property risk assessment completed during the period for a sample of data center facilities to determine that technical operations performed a risk assessment on during the period to identify and analyze the business and security risks, vulnerabilities, laws, and regulations, and the risk assessment also included the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system and risks identified were formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies for each data center facility sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **Monitoring Activities** | | | |
| **CC4.1** COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | | |
| CC4.1.1 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC4.1.2 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| CC4.1.3 **Centralized** | A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. | Inspected the threat and vulnerability management policy and a sample of closed tickets from the ticketing system during the period to determine that a formal threat and vulnerability management process was in place for addressing identified threats and vulnerabilities and findings were remediated according to internal policy SLAs for each ticket sampled. | No exceptions noted. |
| CC4.1.4 **Centralized** | An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. | Inspected the IDS alert report, listing of IDS sensors, and example e-mail alert notifications generated during the period to determine that an IDS was deployed throughout the environment to monitor and prevent malicious activity at the log and network levels and that IT personnel were alerted of events via e-mail notification during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC4.1.5 **Centralized** | External assessments are conducted by an accredited independent third-party assessor on an annual basis. The results of the audits are reviewed by management as part of the management review process. | Inspected an example assessment conducted by an accredited independent third-party assessor to determine that external assessments were conducted by accredited independent third-party assessors on an annual basis, and the results of the audits were reviewed by management as part of the annual management review process. | No exceptions noted. |
| **CC4.2** COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | | | |
| CC4.2.1 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC4.2.2 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| CC4.2.3 **Centralized** | A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. | Inspected the threat and vulnerability management policy and a sample of closed tickets from the ticketing system during the period to determine that a formal threat and vulnerability management process was in place for addressing identified threats and vulnerabilities and findings were remediated according to internal policy SLAs for each ticket sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC4.2.4 **Centralized** | An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. | Inspected the IDS alert report, listing of IDS sensors, and example e-mail alert notifications generated during the period to determine that an IDS was deployed throughout the environment to monitor and prevent malicious activity at the log and network levels and that IT personnel were alerted of events via e-mail notification during the period. | No exceptions noted. |
| CC4.2.5 **Centralized** | External assessments are conducted by an accredited independent third-party assessor on an annual basis. The results of the audits are reviewed by management as part of the management review process. | Inspected an example assessment conducted by an accredited independent third-party assessor to determine that external assessments were conducted by accredited independent third-party assessors on an annual basis, and the results of the audits were reviewed by management as part of the annual management review process. | No exceptions noted. |
| CC4.2.6 **Centralized** | Annual assessments are performed by the compliance team. These assessments include evaluation of the operation of key controls. Assessments are reviewed and require the development of corrective action plans for control weaknesses. | Inspected the most recently completed security standardized assessments for a sample of data center facilities performed during the period to determine that annual assessments were performed by the compliance team, and these assessments included evaluation of the operation of key controls, assessments were reviewed, and required the development of corrective action plans for control weaknesses for each data center facility sampled. | No exceptions noted. |
| **Control Activities** | | | |
| **CC5.1** COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | | |
| CC5.1.1 **Centralized** | Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. | Inspected the risk mitigation policies and example risk mitigation plans to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the annual risk assessment process, and control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC5.2** COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | | |
| CC5.2.1 **Centralized** | Assigned risk owners select and develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. | Inspected the property risk assessment report and example mitigation plans completed during the period for a sample of data center facilities to determine that assigned risk owners selected and developed control activities over technology to support the achievement of objectives as an output from the risk assessment performed during the period. The control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold for each data center facility sampled. | No exceptions noted. |
| CC5.2.2 **Centralized** | Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. | Inspected the risk mitigation policies and example risk mitigation plans completed during the period for a sample of data center facilities to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the annual risk assessment process, and control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold for each data center facility sampled. | No exceptions noted. |
| **CC5.3** COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | | |
| CC5.3.1 **Centralized** | Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the intranet. | Inspected the data center operations policies and procedures to determine that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the intranet. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC5.3.2 **Centralized** | An information system security and management policy/data classification policy are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | Inspected the security policies and management policy/data classification policy displayed on the company intranet to determine that documented policies and procedures were formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | No exceptions noted. |
| CC5.3.3 **Centralized** | Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. | Inspected the code of conduct to determine that policies were documented and maintained that address remedial actions for lack of compliance with policies and procedures. | No exceptions noted. |
| **Logical and Physical Access Controls** | | | |
| **CC6.1** The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | | | |
| CC6.1.1 **Centralized** | Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. | Inspected the security policies and customer handbook displayed on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements were communicated to internal personnel via the company Intranet. | No exceptions noted. |
| CC6.1.2 **Centralized** | The in-scope systems require the authentication of users with a unique user account and enforce predefined user account and minimum password requirements. | Inspected the user account listings and password configurations for a sample of in-scope systems during the period to determine that each in-scope system required the authentication of users with a unique user account and enforced predefined user account and minimum password requirements. | No exceptions noted. |
| CC6.1.3 **Centralized** | Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. | Inspected the user account listing for a sample of in-scope systems during the period to determine that predefined security groups were utilized to assign least privilege based access privileges and segregate access to data for each in-scope system sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.1.4 **Centralized** | Administrative access privileges to the in-scope systems are restricted by user accounts accessible by authorized personnel. | Inspected the administrative user account listings for a sample of in-scope systems during the period with the assistance of the director of global operations compliance to determine that administrative access privileges for each in-scope system was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| **CC6.2** Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | | | |
| CC6.2.1 **Centralized** | User account requests are documented on a standard access request form and require the approval of a manager or delegate. | Inspected user account tickets for a sample of users provided access during the period to determine that internal and external user account requests were documented on a standard access request form and required the approval of a manager or delegate for each user sampled. | No exceptions noted. |
| CC6.2.2 **Centralized** | User access reviews are performed on an annual basis to ensure that access to data was restricted to authorized personnel and provided for segregation of duties. | Inspected the most recent logical access reviews for a sample of data center facilities to determine that an access review was performed during the period to ensure that access to data was restricted to authorized personnel and provided for segregation of duties for each facility sampled. | No exceptions noted. |
| CC6.2.3 **Centralized** | A termination checklist and ticket are completed, and logical access is revoked within timelines established by policy for employees as a component of the employee termination process. | Inspected the termination notification tickets and user listings for a sample of employees terminated during the period for the in-scope systems to determine that a termination notification ticket was completed, and logical access was revoked to the in-scope systems for each terminated employee sampled. | No exceptions noted. |
| **CC6.3** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| CC6.3.1 **Centralized** | User account requests are documented on a standard access request form and require the approval of a manager or delegate. | Inspected user account tickets for a sample of users provided access during the period to determine that internal and external user account requests were documented on a standard access request form and required the approval of a manager or delegate for each user sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.3.2 **Centralized** | User access reviews are performed on an annual basis to ensure that access to data was restricted to authorized personnel and provided for segregation of duties. | Inspected the most recent logical access reviews for a sample of data center facilities to determine that an access review was performed during the period to ensure that access to data was restricted to authorized personnel and provided for segregation of duties for each facility sampled. | No exceptions noted. |
| CC6.3.3 **Centralized** | Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. | Inspected the user account listing for a sample of in-scope systems during the period to determine that predefined security groups were utilized to assign least privilege based access privileges and segregate access to data for each in-scope system sampled. | No exceptions noted. |
| CC6.3.4 **Centralized** | Administrative access privileges to the in-scope systems are restricted by user accounts accessible by authorized personnel. | Inspected the administrative user account listings for a sample of in-scope systems during the period with the assistance of the director of global operations compliance to determine that administrative access privileges for each in-scope system was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| CC6.3.5 **Centralized** | A termination checklist and ticket are completed, and logical access is revoked within timelines established by policy for employees as a component of the employee termination process. | Inspected the termination notification tickets and user listings for a sample of employees terminated during the period for the in-scope systems to determine that a termination notification ticket was completed, and logical access was revoked to the in-scope systems for each terminated employee sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC6.4** The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. | | | |
| CC6.4.1<br>**Site Level** | Physical access controls are in place to restrict access to and within the data center facilities. | Observed the physical access control systems at each data center facility to determine that physical access controls were in place to restrict access to and within the data center facilities that included the following:<br>· Two-factor authentication system for access to the data centers and suites<br>· Personnel entering the data center facility were required to wear badges identifying them as visitor, employee, contractor, or strategic partner<br>· Visitor logs recorded visitor access to the data center facility<br>· Visitors required an escort as needed | No exceptions noted. |
| CC6.4.2<br>**Centralized** | Physical access requests are documented and require the approval of the relevant access authorizer. | Inspected physical access requests for a sample of personnel granted data center access during the period to determine that physical access requests were documented on a standard access request form and were approved by the relevant access authorizer for each user sampled. | No exceptions noted. |
| CC6.4.3<br>**Site Level** | A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed. | Inspected the most recently completed physical access reviews during the period to determine that a review of Digital Realty employees and contractors with physical access to customer suites was performed and unnecessary access was identified, notified, and removed during the period. | No exceptions noted. |
| CC6.4.4<br>**Centralized** | A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. | Inspected the termination notification ticket, access removal ticket, and data center access listings for a sample of employees and contractors terminated during the period to determine that a termination ticket was completed and access was revoked within one business day of notification for each terminated employee and contractor sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC6.4.5 **Site Level** | Escorted visitors are required to surrender their badges at the end of the day. | Observed the visitor access process and inspected the operations procedures to determine that escorted visitors were required to surrender their badges at the end of the day. | No exceptions noted. |
| CC6.4.6 **Site Level** | Surveillance cameras are located along the building perimeters and within the data centers to monitor and record access to and within the data centers. | Observed the surveillance cameras located throughout the data centers to determine that surveillance cameras were in place to monitor and record access along the building perimeters and within the data centers. | No exceptions noted. |
| CC6.4.7 **Site Level** | Digital surveillance systems are configured to retain video footage for the in-scope data center facilities for a minimum of 90 days or maximum allowed by local legislation. | Inspected digital surveillance system images dated during the period for the in-scope data center facilities to determine that digital surveillance systems were configured to retain video footage for the in-scope data centers for a minimum of 90 days or maximum allowed by local legislation. | No exceptions noted. |
| **CC6.5** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| CC6.5.1 **Centralized** | Documented media sanitation policies are in place to guide personnel in the disposal of confidential information stored on media devices. | Inspected the media sanitation policy to determine that documented media sanitation policies were in place to guide personnel in the disposal of confidential information stored on media devices. | No exceptions noted. |
| CC6.5.2 **Centralized** | Requests to dispose of media devices containing confidential information are entered via the ticketing system and disposed. Customers receive a receipt of data destruction upon completion of data disposal. | Inspected an example media disposal ticket during the period to determine that requests to dispose of media devices containing confidential information were entered via the ticketing system and disposed, and customers received a receipt of data destruction upon completion of data disposal. | No exceptions noted. |
| **CC6.6** The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | | |
| Not Applicable – The Digital Realty in-scope systems do not transmit, move, or remove data outside the boundaries of the system and Digital Realty does not administer logical access to systems for user entities. | | | |
| **CC6.7** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| Not Applicable – The Digital Realty in-scope systems do not transmit, move, or remove data outside the boundaries of the system and Digital Realty does not administer logical access to systems for user entities. | | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **CC6.8** The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | | | |
| CC6.8.1 **Centralized** | A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. | Inspected the threat and vulnerability management policy and a sample of closed tickets from the ticketing system during the period to determine that a formal threat and vulnerability management process was in place for addressing identified threats and vulnerabilities and findings were remediated according to internal policy SLAs for each ticket sampled. | No exceptions noted. |
| CC6.8.2 **Centralized** | An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. | Inspected the IDS alert report, listing of IDS sensors, and example e-mail alert notifications generated during the period to determine that an IDS was deployed throughout the environment to monitor and prevent malicious activity at the log and network levels and that IT personnel were alerted of events via e-mail notification during the period. | No exceptions noted. |
| **System Operations** | | | |
| **CC7.1** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | | |
| CC7.1.1 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC7.1.2 **Centralized** | An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. | Inspected the IDS alert report, listing of IDS sensors, and example e-mail alert notifications generated during the period to determine that an IDS was deployed throughout the environment to monitor and prevent malicious activity at the log and network levels and that IT personnel were alerted of events via e-mail notification during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC7.1.3 **Centralized** | Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization, and alert the information security team upon detection of usual system activity or service requests. | Inspected the monitoring applications notification configurations and example e-mail alert notifications generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems and alert the information security team upon detection of usual system activity or service requests. | No exceptions noted. |
| CC7.1.4 **Centralized** | A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. | Inspected the threat and vulnerability management policy and a sample of closed tickets from the ticketing system during the period to determine that a formal threat and vulnerability management process was in place for addressing identified threats and vulnerabilities and findings were remediated according to internal policy SLAs for each ticket sampled. | No exceptions noted. |
| **CC7.2** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | | | |
| CC7.2.1 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC7.2.2 **Centralized** | An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. | Inspected the IDS alert report, listing of IDS sensors, and example e-mail alert notifications generated during the period to determine that an IDS was deployed throughout the environment to monitor and prevent malicious activity at the log and network levels and that IT personnel were alerted of events via e-mail notification during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC7.2.3 **Centralized** | Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization, and alert the information security team upon detection of usual system activity or service requests. | Inspected the monitoring applications notification configurations and example e-mail alert notifications generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems and alert the information security team upon detection of usual system activity or service requests. | No exceptions noted. |
| CC7.2.4 **Centralized** | A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. | Inspected the threat and vulnerability management policy and a sample of closed tickets from the ticketing system during the period to determine that a formal threat and vulnerability management process was in place for addressing identified threats and vulnerabilities and findings were remediated according to internal policy SLAs for each ticket sampled. | No exceptions noted. |
| **CC7.3** The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | | | |
| CC7.3.1 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| CC7.3.2 **Centralized** | Incident response procedures are in place that outline the response procedures to security events and includes lessons learned to evaluate the effectiveness of the procedures. The procedures are reviewed on an annual basis to ensure they are effectively meeting the business objectives. | Inspected the security incident procedures to determine that incident response procedures were in place that outlined the response procedures to security events and included lessons learned to evaluate the effectiveness of the procedures, and the procedures were reviewed on an annual basis to help ensure they were effectively meeting the business objectives. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC7.3.3 **Centralized** | Security personnel utilize an automated ticketing system to document security violations, responses, and resolution. | Inspected the incident ticket for a sample of closed incident tickets during the period from the incident ticketing system to determine that an automated ticketing system was utilized to document security violations, responses, and resolution for each incident ticket sampled. | No exceptions noted. |
| CC7.3.4 **Centralized** | Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process. | Inspected the change ticket for a sample of closed incidents during the period from the incident ticketing system to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process for each incident ticket sampled. | No exceptions noted. |
| **CC7.4** The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| CC7.4.1 **Centralized** | Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | Inspected the security incident procedures displayed internally on the company intranet and the externally available customer handbook to determine that documented escalation procedures for reporting security and availability incidents were provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| CC7.4.2 **Centralized** | Roles and responsibilities are assigned for the design, implementation, maintenance, and execution of the security incident management process. | Inspected the security incident procedures to determine that roles and responsibilities were assigned for the design, implementation, maintenance, and execution of the security incident management process. | No exceptions noted. |
| CC7.4.3 **Centralized** | Reported or detected security incidents are tracked within a ticketing system until resolved. Closed security incidents are reviewed and approved by management to ensure that the incident response procedures were followed, and that the incident was resolved. | Inspected the security incident ticket for a sample of security incidents detected during the period to determine that reported or detected security incidents were tracked within a ticketing system until resolved and that closed security incidents were reviewed and approved by management to ensure that the incident response procedures were followed, and that the incident was resolved for each security incident ticket sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC7.4.4 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| **CC7.5** The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| CC7.5.1 **Centralized** | Documented policies and procedures are in place to guide personnel in the identification, reporting, and resolution of system security breaches and other incidents. | Inspected the security incident procedures to determine that documented policies and procedures were in place to guide personnel in the identification, reporting, and resolution of system security breaches and other incidents. | No exceptions noted. |
| CC7.5.2 **Centralized** | Security personnel utilize an automated ticketing system to document security violations, responses, and resolution. | Inspected the incident ticket for a sample of closed incident tickets during the period from the incident ticketing system to determine that an automated ticketing system was utilized to document security violations, responses, and resolution for each incident ticket sampled. | No exceptions noted. |
| CC7.5.3 **Centralized** | Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. | Inspected the management meeting calendar invite and meeting minutes for a sample of months during the period to determine that management meetings were held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures for each month sampled. | No exceptions noted. |
| CC7.5.4 **Centralized** | Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process. | Inspected the change ticket for a sample of closed incidents during the period from the incident ticketing system to determine that corrective measures or changes that occurred as a result of incidents and identified deficiencies followed the standard change control process for each incident ticket sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **Change Management** | | | |
| **CC8.1** The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | | | |
| CC8.1.1 **Centralized** | Documented policies and procedures are in place to guide personnel in the release management and change management process. | Inspected the change management policies displayed on the company Intranet to determine that documented policies and procedures were in place to guide personnel in the release management and change management process. | No exceptions noted. |
| CC8.1.2 **Centralized** | A change management meeting is held on a monthly basis to discuss and communicate the past, ongoing, and upcoming projects that affect the system. | Inspected the change management recurring meeting invitation and example meeting minutes for a sample of months during the period to determine that a change management meeting was held to discuss and communicate the past, ongoing, and upcoming projects that affect the system for each month sampled. | No exceptions noted. |
| CC8.1.3 **Centralized** | Changes to network devices are logged, tested where applicable, approved, and closed in a timely manner. | Inspected the CRM tickets for a sample of network device changes implemented during the period to determine that each change sampled was logged, tested where applicable, approved, and closed in a timely manner. | No exceptions noted. |
| CC8.1.4 **Centralized** | Requests for changes, system maintenance, and supplier maintenance are documented, prioritized, tested, and approved. | Inspected the CRM tickets for a sample of changes, system maintenance, and supplier maintenance requests to determine that each sampled request for changes, system maintenance, and supplier maintenance were documented, prioritized, tested, and approved. | No exceptions noted. |
| **Risk Mitigation** | | | |
| **CC9.1** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| CC9.1.1 **Centralized** | An insurance policy is in place covering commercial and professional liability to offset the financial impact of materializing risk. | Inspected the insurance policy to determine that an insurance policy was in place covering commercial and professional liability to offset the financial impact of materializing risk. | No exceptions noted. |
| CC9.1.2 **Centralized** | Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. | Inspected the emergency recovery plan to determine that emergency recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| CC9.1.3 **Centralized** | Risk mitigation policies and procedures are in place to guide personnel in the development and deployment of risk mitigation strategies. | Inspected the risk assessment policy to determine that policies and procedures were in place to guide personnel in the development and deployment of risk mitigation strategies. | No exceptions noted. |
| **CC9.2** The entity assesses and manages risks associated with vendors and business partners. | | | |
| CC9.2.1 **Centralized** | A vendor management policy is in place that addresses specific requirements for a vendor and the supporting monitoring and review process. | Inspected the vendor management policy to determine that a vendor management policy was in place that addressed specific requirements for a vendor and the supporting monitoring and review process. | No exceptions noted. |
| CC9.2.2 **Centralized** | The entity's established vendor requirements, scope of services, roles, and responsibilities and service levels are documented in vendor contracts. | Inspected the vendor contracts for a sample of vendors active during the period to determine that the entity's established vendor requirements, scope of services, roles, and responsibilities and service levels were documented in vendor contracts for each vendor sampled. | No exceptions noted. |
| CC9.2.3 **Centralized** | Management performs service reviews of third-party vendors on an at least an annual basis to help ensure that third party vendors maintain compliance with security and availability commitments. | Inspected the vendor risk assessments for a sample of vendors during the period to determine that management performed service reviews of third-party vendors during the period to help ensure that third-party vendors maintained compliance with security and availability commitments for each vendor sampled. | No exceptions noted. |

## Additional Criteria for Availability

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **A1.1** The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | | | |
| A1.1.1 **Site Level** | BMS applications are configured to monitor environmental systems and alert the facility team when predefined thresholds have been met. | Inspected the BMS application configurations and example notifications generated during the period to determine that BMS applications were configured to monitor environmental systems and alert IT personnel when predefined thresholds were met. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| A1.1.2 **Centralized** | Management meetings are held on at least a quarterly basis to review availability trends and availability forecasts as compared to system requirements. | Inspected the management calendar invite and meeting minutes for a sample of quarters during the period to determine that management meetings were held on a quarterly basis to review availability trends and availability forecasts as compared to system requirements for each quarter sampled. | No exceptions noted. |
| **A1.2** The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| A1.2.1 **Site Level** | BMS applications are configured to monitor environmental systems and alert the facility team when predefined thresholds have been met. | Inspected the BMS application configurations and example notifications generated during the period to determine that BMS applications were configured to monitor environmental systems and alert IT personnel when predefined thresholds were met. | No exceptions noted. |
| A1.2.2 **Centralized** | Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. | Inspected the emergency recovery plan to determine that emergency recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. | No exceptions noted. |
| A1.2.3 **Site Level** | The data centers are equipped with the following environmental protection equipment:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems | Observed the environmental systems at the data center facilities to determine that the data centers were equipped with the following environmental protection equipment:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems | No exceptions noted. |
| A1.2.4 **Site Level** | Management retains the inspection report received from third party specialists evidencing completion of inspection and maintenance of the following on at least an annual basis:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems | Inspected the preventative maintenance reports associated with the preventative maintenance calendar to determine that the following equipment was inspected during the period:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems | No exceptions noted. |
| A1.2.5 **Site Level** | Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring. | Inspected the security post orders to determine that site security personnel were assigned daily operational procedures and tasks that included environmental system monitoring. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| **A1.3** The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |
| A1.3.1 **Centralized** | Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. | Inspected the emergency recovery plan to determine that emergency recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. | No exceptions noted. |
| A1.3.2 **Centralized** | The operational site team performs an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements. | Inspected the results from the most recently completed recovery tests performed during the period for a sample of data center facilities to determine that disaster recovery personnel performed an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements for each facility sampled. | No exceptions noted. |

# SECTION 5

## OTHER INFORMATION PROVIDED BY DIGITAL REALTY

# NIST 800-53 Rev 5 Control Mapping

The following mapping is provided for information purposes and maps the Digital Realty SOC 2 controls to the applicable NIST Special Publication (SP) 800-53 revision 5 physical and environmental control family requirements at the moderate baseline.

**Physical and Environmental Protection (PE)**

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

| NIST 800-53 Physical and Environmental Protection (PE) Control Categories | Related Digital Realty Controls |
|---|---|
| PE-1: Physical and Environmental Protection Policy and Procedures | CC2.3.5: The director of site operations performs an annual review of the Digital Realty security post orders including system security changes that might impact local property teams. The approved post orders are disseminated to the local site management by site operations. |
| | CC3.1.2, CC.3.2.1, & CC3.4.2: Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. |
| | CC5.2.1: Assigned risk owners select and develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. |
| | CC6.5.1: Documented media sanitation policies are in place to guide personnel in the disposal of confidential information stored on media devices. |
| | CC9.1.3: Risk mitigation policies and procedures are in place to guide personnel in the development and deployment of risk mitigation strategies. |
| PE-2: Physical Access Authorizations | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| | CC6.4.3: A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed. |
| | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |
| PE-3: Physical Access Control | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | CC6.4.6: Surveillance cameras are located along the building perimeters and within the data centers to monitor and record access to and within the data centers. |
| | CC6.4.7: Digital surveillance systems are configured to retain video footage for the in-scope data center facilities for a minimum of 90 days or maximum allowed by local legislation. |
| PE-4: Access Control for Transmission | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| PE-5: Access Control for Output Devices | Refer to PE-4 controls noted above. |

| NIST 800-53 Physical and Environmental Protection (PE) Control Categories | Related Digital Realty Controls |
|---|---|
| PE-6: Monitoring Physical Access | A1.1.1 & A1.2.1: BMS applications are configured to monitor environmental systems and alert the facility team when predefined thresholds have been met. |
| | CC2.1.3: Security management systems are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. |
| | CC2.1.4 & CC3.2.3: Security staff continuously monitors the security management system in real-time that captures card activity of access points to the Building and access points to the Suites. Security staff acknowledge the logged exception events to evidence resolution. |
| | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | CC6.4.6: Surveillance cameras are located along the building perimeters and within the data centers to monitor and record access to and within the data centers. |
| | CC6.4.7: Digital surveillance systems are configured to retain video footage for the in-scope data center facilities for a minimum of 90 days or maximum allowed by local legislation. |
| | CC7.3.3 & CC7.5.2: Security personnel utilize an automated ticketing system to document security violations, responses, and resolution. |
| | CC7.4.3: Reported or detected security incidents are tracked within a ticketing system until resolved. Closed security incidents are reviewed and approved by management to ensure that the incident response procedures were followed, and that the incident was resolved. |
| PE-6(1): Monitoring Physical Access \| Intrusion Alarms and Surveillance Equipment | CC6.4.6: Surveillance cameras are located along the building perimeters and within the data centers to monitor and record access to and within the data centers. |
| PE-8: Visitor Access Records | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| PE-9: Power Equipment and Cabling | A1.1.1 & A1.2.1: BMS applications are configured to monitor environmental systems and alert the facility team when predefined thresholds have been met. |
| | A1.2.3: The data centers are equipped with the following environmental protection equipment:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |
| PE-10: Emergency Shutoff | Refer to the PE-9 controls noted above. |
| | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| PE-11: Emergency Power | Refer to the PE-9 controls noted above. |
| PE-12: Emergency Lighting | Refer to the PE-9 controls noted above. |
| PE-13: Fire Protection | Refer to the PE-9 controls noted above. |
| PE-13(1): Fire Protection \| Detection Systems – Automatic Activation and Notification | Refer to the PE-9 controls noted above. |
| PE-14: Environmental Controls | Refer to the PE-9 controls noted above. |
| | A1.2.5: Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring. |
| PE-15: Water Damage Protection | Refer to the PE-9 controls noted above. |

| NIST 800-53 Physical and Environmental Protection (PE) Control Categories | Related Digital Realty Controls |
|---|---|
| PE-16: Delivery and Removal | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| | CC6.4.6: Surveillance cameras are located along the building perimeters and within the data centers to monitor and record access to and within the data centers. |
| | CC6.4.7: Digital surveillance systems are configured to retain video footage for the in-scope data center facilities for a minimum of 90 days or maximum allowed by local legislation. |
| | CC6.5.1: Documented media sanitation policies are in place to guide personnel in the disposal of confidential information stored on media devices. |
| PE-17: Alternate Work Site | CC1.2.4: The BoD meets on an annual basis to review and approve strategic company objectives and the performance of internal control. |
| | CC1.5.2: Management provides internal control performance metrics and third-party audit results to the BoD on an annual basis. |
| | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| | A1.3.2: The operational site team performs an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements. |

# HIPAA/HITECH Control Mapping

The following mapping is provided for information purposes and maps the Digital Realty SOC 2 controls to the HIPAA Security and Breach Notification Rules.

### Security Rule

| §164.306 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | **Covered entities and business associates must do the following:** | |
| (a)(1) | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| (a)(2) | Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. | CC2.1.2, CC4.1.3, CC4.2.3, CC6.8.1, CC7.1.4, & CC7.2.4: A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. |

| §164.306 | Requirement | Related Digital Realty Control |
|---|---|---|
| | | CC2.1.4 & CC3.2.3: Security staff continuously monitors the security management system in real-time that captures card activity of access points to the Building and access points to the Suites. Security staff acknowledge the logged exception events to evidence resolution. |
| (a)(3) | Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(4) | Ensure compliance with this subpart by its workforce. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| (b) | **Flexibility of approach:** | |
| (b)(1) | Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| (b)(2)(i) | In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |

| §164.306 | Requirement | Related Digital Realty Control |
|---|---|---|
| (b)(2)(ii) | The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| (b)(2)(iii) | The costs of security measures. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| (b)(2)(iv) | The probability and criticality of potential risks to electronic protected health information. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |

| §164.308 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | **A covered entity or business associate must, in accordance with § 164.306:** | |
| (a)(1)(i) | **Standard: Security Management Process.** Implement policies and procedures to prevent, detect, contain, and correct security violations. | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |

| §164.308 | Requirement | Related Digital Realty Control |
| --- | --- | --- |
| (a)(1)(ii) | **Implementation Specifications:** | |
| (a)(1)(ii)(A) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| (a)(1)(ii)(B) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a). | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| (a)(1)(ii)(C) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity’s security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| (a)(1)(ii)(D) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | CC2.1.4 & CC3.2.3: Security staff continuously monitors the security management system in real-time that captures card activity of access points to the Building and access points to the Suites. Security staff acknowledge the logged exception events to evidence resolution. |

| §164.308 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a)(2) | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. | CC1.3.3: Management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team. |
| (a)(3)(i) | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(3)(ii) | **Implementation Specifications:** | |
| (a)(3)(ii)(A) | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(3)(ii)(B) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(3)(ii)(C) | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b). | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(4)(i) | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(4)(ii) | **Implementation Specifications:** | |
| (a)(4)(ii)(A) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | **Not applicable**. DLR is not a clearing house. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(4)(ii)(B) | Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | **Not applicable**. DLR is not a clearing house. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(4)(ii)(C) | Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(5)(i) | Implement a security awareness and training program for all members of its workforce (including management). | CC1.4.3 & CC2.2.2: Operations employees are required to complete security awareness training, upon hire, and annually, to understand their obligations, and responsibilities to comply with the corporate and business unit security policies. |

| §164.308 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a)(5)(ii) | **Implementation Specifications:** | |
| (a)(5)(ii)(A) | Periodic security updates. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(5)(ii)(B) | Procedures for guarding against, detecting, and reporting malicious software. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(5)(ii)(C) | Procedures for monitoring log-in attempts and reporting discrepancies. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(5)(ii)(D) | Procedures for creating, changing, and safeguarding passwords. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(6)(i) | Implement policies and procedures to address security incidents. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(6)(ii) | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(7)(i) | Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| | | A1.3.2: The operational site team performs an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements. |
| (a)(7)(ii) | **Implementation Specifications:** | |
| (a)(7)(ii)(A) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(7)(ii)(B) | Establish (and implement as needed) procedures to restore any loss of data. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(7)(ii)(C) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(7)(ii)(D) | Implement procedures for periodic testing and revision of contingency plans. | A1.3.2: The operational site team performs an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements. |

| §164.308 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a)(7)(ii)(E) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(8) | Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. | CC3.1.2, CC.3.2.1, & CC3.4.2: Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. |
| | | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| (b)(1) | A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. | **Not applicable.** Digital Realty is not a covered entity. |
| (b)(2) | A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information. | **Not applicable**. Digital Realty generally has very limited access to customer data and does not share data with other providers. |
| (b)(3) | Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a). | **Not applicable**. Digital Realty generally has very limited access to customer data and does not share data with other providers. |

| §164.310 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | **A covered entity or business associate must, in accordance with § 164.306:** | |
| (a)(1) | **Standard: Facility access controls.** Implement policies and procedures to limit physical access to [an entity's] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| | | CC6.4.3: A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed. |
| | | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |
| | | CC6.4.5: Escorted visitors are required to surrender their badges at the end of the day. |
| (a)(2) | **Implementation Specifications:** | |
| (a)(2)(i) | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| | | A1.3.2: The operational site team performs an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements. |
| (a)(2)(ii) | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| | | CC6.4.3: A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed. |
| | | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |
| | | CC6.4.5: Escorted visitors are required to surrender their badges at the end of the day. |

| §164.310 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a)(2)(iii) | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| | | CC6.4.3: A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed. |
| | | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |
| | | CC6.4.5: Escorted visitors are required to surrender their badges at the end of the day. |
| (a)(2)(iv) | Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | CC8.1.3: Changes to network devices are logged, tested where applicable, approved, and closed in a timely manner. |
| | | CC8.1.4: Requests for changes, system maintenance, and supplier maintenance are documented, prioritized, tested, and approved. |
| (b) | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | **Not applicable.** Protected health information is not stored or processed on Digital Realty workstations. |
| (c) | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | **Not applicable.** Protected health information is not stored or processed on Digital Realty workstations. |
| (d)(1) | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility. | **Not applicable.** Protected health information is not stored or processed on Digital Realty workstations. |
| (d)(2) | **Implementation Specifications:** | |
| (d)(2)(i) | Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored. | **Not applicable**. Device and media controls addressing the final disposal of ePHI are the responsibility of Digital Realty's customers. |
| (d)(2)(ii) | Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. | **Not applicable**. Device and media controls addressing the final disposal of ePHI are the responsibility of Digital Realty's customers. |
| (d)(2)(iii) | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | CC6.5.2: Requests to dispose of media devices containing confidential information are entered via the ticketing system and disposed. Customers receive a receipt of data destruction upon completion of data disposal. |

| §164.310 | Requirement | Related Digital Realty Control |
|---|---|---|
| (d)(2)(iv) | Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |

| §164.312 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | **A covered entity or business associate must, in accordance with § 164.306:** | |
| (a)(1) | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). | **Not applicable.** Protected health information is not stored or processed on Digital Realty workstations. |
| (a)(2) | **Implementation Specifications:** | |
| (a)(2)(i) | Assign a unique name and/or number for identifying and tracking user identity. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(2)(ii) | Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(2)(iii) | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (a)(2)(iv) | Implement a mechanism to encrypt and decrypt electronic protected health information. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (b) | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (c)(1) | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | **Not applicable**. Device and media controls addressing the final disposal of ePHI are the responsibility of Digital Realty's customers. |
| (c)(2) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (d) | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (e)(1) | Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (e)(2) | **Implementation Specifications:** | |
| (e)(2)(i) | Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |

| §164.312 | Requirement | Related Digital Realty Control |
|---|---|---|
| (e)(2)(ii) | Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |

| §164.314 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a)(1) | The contract or other arrangement between the covered entity and its business associate required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(2)(i)(A) | The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart. | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(2)(i)(B) | The contract must provide that the business associate will, in accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section. | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(2)(i)(C) | The contract must provide that the business associate will report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by §164.410. | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(2)(ii) | The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3). | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(2)(iii): | The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(b)(1) | Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | **Not applicable**. Digital Realty is not a group health plan. |
| (b)(2)(i) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan. | **Not applicable**. Digital Realty is not a group health plan. |

| §164.314 | Requirement | Related Digital Realty Control |
|---|---|---|
| (b)(2)(ii) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures. | **Not applicable**. Digital Realty is not a group health plan. |
| (b)(2)(iii) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information. | **Not applicable**. Digital Realty is not a group health plan. |
| (b)(2)(iv) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware. | **Not applicable**. Digital Realty is not a group health plan. |

| §164.316 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | CC1.1.2: Management formally documents and reviews organizational updates that communicate entity values and behavioral standards to personnel on an annual basis. |
| (b)(1)(i) | Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| (b)(1)(ii) | If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record or the action, activity, or assessment. | CC1.1.2: Management formally documents and reviews organizational updates that communicate entity values and behavioral standards to personnel on an annual basis. |
| (b)(2)(i) | Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (b)(2)(ii) | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |

| §164.316 | Requirement | Related Digital Realty Control |
|---|---|---|
| (b)(2)(iii) | Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. | CC1.1.2: Management formally documents and reviews organizational updates that communicate entity values and behavioral standards to personnel on an annual basis. |

### Breach Notification Rule

| §164.414 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | Administrative Requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule"). [Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and documentation] | **Not applicable**. Digital Realty is not a covered entity. |

| §164.530 | Requirement | Related Digital Realty Control |
|---|---|---|
| (b) | Training. All workforce members must receive training pertaining to the Breach Notification Rule. | **Not applicable**. Digital Realty is not a covered entity. |
| (d) | Complaints. All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule. | **Not applicable**. Digital Realty is not a covered entity. |
| (e) | Sanctions. All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule. | **Not applicable**. Digital Realty is not a covered entity. |
| (g) | Refraining from Retaliatory Acts. All covered entities must have policies and procedures in place to prohibit retaliatory acts. | **Not applicable**. Digital Realty is not a covered entity. |
| (h) | Waiver of Rights. All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits. | **Not applicable**. Digital Realty is not a covered entity. |
| (i) | Policies and Procedures. All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule. | **Not applicable**. Digital Realty is not a covered entity. |
| (j) | Documentation. All covered entities must have policies and procedures in place for maintaining documentation. | **Not applicable**. Digital Realty is not a covered entity. |

| §164.402 | Requirement | Related Digital Realty Control |
|---|---|---|
| | Definitions: Breach Exceptions - Unsecured PHI. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;(ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and(iv) The extent to which the risk to the PHI has been mitigated. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |

| §164.404 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a)(1) | Notice to Individuals. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. | **Not applicable**. Digital Realty is not a covered entity. |
| (a)(2) | Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency). | **Not applicable**. Digital Realty is not a covered entity. |
| (b) | Timeliness of Notifications. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. | **Not applicable**. Digital Realty is not a covered entity. |

| §164.404 | Requirement | Related Digital Realty Control |
|---|---|---|
| (c)(1) | Content of Notification. The notification required by paragraph (a) of this section shall include, to the extent possible:(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);(C) Any steps the individual should take to protect themselves from potential harm resulting from the breach;(D) A brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.(2) The notification required by paragraph (a) of this section shall be written in plain language. | **Not applicable**. Digital Realty is not a covered entity. |
| (d) | Methods of Notification. The notification required by paragraph (a) of this section shall be provided in the following form: | |
| (d)(1)(i) | Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information becomes available. | **Not applicable**. Digital Realty is not a covered entity. |

| §164.404 | Requirement | Related Digital Realty Control |
|---|---|---|
| (d)(1)(ii) | If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual is required. The notification may be provided in one or more mailings as information is available. (2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone, or other means.(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.(3) In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section. | **Not applicable**. Digital Realty is not a covered entity. |

| §164.406 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | Notification to the Media. For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.(b)Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.(c) The content of the notification required by paragraph (a) of this section shall meet the requirements of §164.404(c). | **Not applicable**. Digital Realty is not a covered entity. |

| §164.408 | Requirement | Related Digital Realty Control |
|---|---|---|
| | **Notification to the Secretary:** | |
| (a) | A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary. (b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site. | **Not applicable**. Digital Realty is not a covered entity. |
| (c) | For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site. | **Not applicable**. Digital Realty is not a covered entity. |

| §164.410 | Requirement | Related Digital Realty Control |
|---|---|---|
| (a) | **Standard:** | |
| (a)(1) | **General Rule.** A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| | | CC.7.3.3 & CC7.5.2: Security personnel utilize an automated ticketing system to document security violations, responses, and resolution. |
| (a)(2) | **Breaches treated as discovered**. For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency). | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| | **Implementation Specifications:** | |
| (b) | **Timeliness of notification**. Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. | CC9.2.2: The entity's established vendor requirements, scope of services, roles, and responsibilities and service levels are documented in vendor contracts. |

| §164.410 | Requirement | Related Digital Realty Control |
|---|---|---|
| (c)(1) | **Content of notification.** (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. | **Not applicable**. Digital Realty does not have access to customer systems or data. Digital Realty customers are responsible for meeting this control requirement. |
| (c)(2) | A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available. | CC.7.3.3 & CC7.5.2: Security personnel utilize an automated ticketing system to document security violations, responses, and resolution. |

| §164.412 | Requirement | Related Digital Realty Control |
|---|---|---|
| | Law Enforcement Delay. If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time. | CC7.5.1: Documented policies and procedures are in place to guide personnel in the identification, reporting, and resolution of system security breaches and other incidents. |

| §164.414 | Requirement | Related Digital Realty Control |
|---|---|---|
| (b) | Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by the subpart or that the use or disclosure did not constitute a breach as defined at §164.402. | **Not applicable**. Digital Realty is not a covered entity. |

# ISO 27002 Annex A Control Mapping

The following mapping is provided for information purposes and maps the Digital Realty SOC 2 controls to the ISO 27002 Annex A Controls.

### A5.1 – Management Direction for Information Security

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.5.1.1 | Policies for information security | A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| | | | CC1.3.1: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| | | | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.5.1.2 | Review of the policies for information security | The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. | CC1.1.2: Management formally documents and reviews organizational updates that communicate entity values and behavioral standards to personnel on an annual basis. |
| | | | CC1.3.1: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. |

**A6.1 – Organization for Information Security**

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.6.1.1 | Information security roles and responsibilities | All information security responsibilities shall be defined and allocated. | CC1.3.1: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. |
| | | | CC1.3.2, CC1.4.5, CC1.5.1, & CC2.2.4: Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. |
| | | | CC1.3.3: Management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team. |
| A.6.1.2 | Segregation of duties | Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuses of the organization's assets. | CC1.3.1: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| | | | CC1.3.2, CC1.4.5, CC1.5.1, & CC2.2.4: Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. |
| A.6.1.3 | Contact with authorities | Appropriate contacts with relevant authorities shall be maintained. | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| A.6.1.4 | Contact with special interest groups | Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. | Digital Realty SOC 2 control does not map back to this control. |
| A.6.1.5 | Information security in project management | Information security shall be addressed in project management, regardless of the type of the project. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |

### A6.2 – Mobile Devices and Teleworking

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.6.2.1 | Mobile device policy | A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| A.6.2.2 | Teleworking | A policy and supporting security measures shall be implemented to protect information access, process or stored at teleworking sites. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |

**A7.1 – Prior To Employment**

To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.7.1.1 | Screening | Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.1.6: Background checks are performed for employees as a component of the hiring process, to the extent permissible by local law. |
| A.7.1.2 | Terms and conditions of employment | The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.3.2, CC1.4.5, CC1.5.1, & CC2.2.4: Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. |
| | | | CC1.4.3 & CC2.2.2: Operations employees are required to complete security awareness training, upon hire, and annually, to understand their obligations, and responsibilities to comply with the corporate and business unit security policies. |
| | | | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |

### A.7.2 – During Employment

To ensure that employees and contractors are aware of and fulfill their information security responsibilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.7.2.1 | Management responsibilities | Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| | | | CC1.3.3: Management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team. |
| A.7.2.2 | Information security awareness, education, and training | All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. | CC1.4.2: Training courses are available to new and existing employees to maintain and advance the skill level of personnel. |
| | | | CC1.4.3 & CC2.2.2: Operations employees are required to complete security awareness training, upon hire, and annually, to understand their obligations, and responsibilities to comply with the corporate and business unit security policies. |
| | | | CC1.4.4 & CC2.2.3: Management monitors compliance with training requirements on an annual basis. |
| A.7.2.3 | Disciplinary process | There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |

### A.7.3 – Termination or Change of Employment

To protect the organization's interests as part of the process of changing or terminating employment.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.7.3.1 | Termination or change of employment responsibilities | Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced. | CC6.2.3 & CC.6.3.5: A termination checklist and ticket are completed, and logical access is revoked within timelines established by policy for employees as a component of the employee termination process. |
| | | | CC.6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |

### A.8.1 – Responsibility for Assets

To identify organizational assets and define appropriate protection responsibilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.8.1.1 | Inventory of assets | Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. | Digital Realty SOC 2 control does not map back to this control. |
| A.8.1.2 | Ownership of assets | Assets maintained in the inventory shall be owned. | Digital Realty SOC 2 control does not map back to this control. |
| A.8.1.3 | Acceptable use of assets | Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | | CC1.3.2, CC1.4.5, CC1.5.1, & CC2.2.4: Position descriptions are documented for full-time employees and include the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.8.1.4 | Return of assets | All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract, or agreement. | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |

### A.8.2 – Information Classification

To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.8.2.1 | Classification of information | Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. | CC5.3.2: An information system security and management policy/data classification policy are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. |
| A.8.2.2 | Labeling of information | An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. | Digital Realty SOC 2 control does not map back to this control. |
| A.8.2.3 | Handling of assets | Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. | Digital Realty SOC 2 control does not map back to this control. |

### A.8.3 – Media Handling

To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.8.3.1 | Management of removable media | Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. | Digital Realty SOC 2 control does not map back to this control. |
| A.8.3.2 | Disposal of media | Media shall be disposed of securely when no longer required, using formal procedures. | CC6.5.1: Documented media sanitation policies are in place to guide personnel in the disposal of confidential information stored on media devices. |
| | | | CC6.5.2: Requests to dispose of media devices containing confidential information are entered via the ticketing system and disposed. Customers receive a receipt of data destruction upon completion of data disposal. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.8.3.3 | Physical media transfer | Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation. | Digital Realty SOC 2 control does not map back to this control. |

### A.9.1 – Business Requirements of Access Control

To limit access to information and information processing facilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.9.1.1 | Access control policy | An access control policy shall be established, documented, and reviewed based on business and information security requirements. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | | CC1.1.5, CC1.5.4, & CC5.3.3: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| | | | CC5.3.2: An information system security and management policy/data classification policy are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. |
| | | | CC6.1.3 & CC6.3.3: Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. |
| | | | CC6.1.4 & CC6.3.4: Administrative access privileges to the in-scope systems are restricted by user accounts accessible by authorized personnel. |
| | | | CC6.2.1 & CC6.3.1: User account requests are documented on a standard access request form and require the approval of a manager or delegate. |
| A.9.1.2 | Access to network and network services | Users shall only be provided with access to the network and network services that they have been specifically authorized to use. | CC6.1.3 & CC6.3.3: Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. |
| | | | CC6.1.4 & CC6.3.4: Administrative access privileges to the in-scope systems are restricted by user accounts accessible by authorized personnel. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| | | | CC6.2.1 & CC6.3.1: User account requests are documented on a standard access request form and require the approval of a manager or delegate. |

**A.9.2 – User Access Management**

To ensure authorized user access and to prevent unauthorized access to systems and services.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.9.2.1 | User registration and de-registration | A formal user registration and de-registration process shall be implemented to enable assignment of access rights. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC6.2.1 & CC6.3.1: User account requests are documented on a standard access request form and require the approval of a manager or delegate. |
| | | | CC6.2.3 & CC.6.3.5: A termination checklist and ticket are completed, and logical access is revoked within timelines established by policy for employees as a component of the employee termination process. |
| | | | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| | | | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |
| A.9.2.2 | User access provisioning | A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC6.2.1 & CC6.3.1: User account requests are documented on a standard access request form and require the approval of a manager or delegate. |
| | | | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| | | | CC6.4.4: A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of notification. |
| A.9.2.3 | Management of privileged access rights | The allocation and use of privileged access rights shall be restricted and controlled. | CC6.1.3 & CC6.3.3: Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. |
| | | | CC6.1.4 & CC6.3.4: Administrative access privileges to the in-scope systems are restricted by user accounts accessible by authorized personnel. |
| A.9.2.4 | Management of secret authentication information of users | The allocation of secret authentication information shall be controlled through a formal management process. | CC6.1.2: The in-scope systems require the authentication of users with a unique user account and enforce predefined user account and minimum password requirements. |
| A.9.2.5 | Review of user access rights | Asset owners shall review users' access rights at regular intervals. | CC6.2.2 & CC6.3.2: User access reviews are performed on an annual basis to ensure that access to data was restricted to authorized personnel and provided for segregation of duties. |
| | | | CC6.4.3: A review of Digital Realty employees and contractors with physical access to customer suites is performed on at least an annual basis and unnecessary access is identified, notified, and removed. |
| A.9.2.6 | Removal or adjustment of access rights | The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change. | CC6.1.8: A termination notification ticket is completed, and logical access is revoked for employees as a component of the employee termination process. |

### A.9.3 – User Responsibilities

To make users accountable for safeguarding their authentication information.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.9.3.1 | Use of secret authentication information | Users shall be required to follow the organization's practices in the use of secret authentication information. | CC6.1.2: The in-scope systems require the authentication of users with a unique user account and enforce predefined user account and minimum password requirements. |

### A.9.4 – System and Application Access Control

To prevent unauthorized access to systems and application.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.9.4.1 | Information access restriction | Access to information and application system functions shall be restricted in accordance with the access control policy. | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| A.9.4.2 | Secure log-on procedures | Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. | CC6.1.2: The in-scope systems require the authentication of users with a unique user account and enforce predefined user account and minimum password requirements. |
| A.9.4.3 | Password management system | Password management systems shall be interactive and shall ensure quality passwords. | CC6.1.2: The in-scope systems require the authentication of users with a unique user account and enforce predefined user account and minimum password requirements. |
| A.9.4.4 | Use of privileged utility programs | The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. | CC6.1.3 & CC6.3.3: Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. |
| | | | CC6.1.4 & CC6.3.4: Administrative access privileges to the in-scope systems are restricted by user accounts accessible by authorized personnel. |
| A.9.4.5 | Access control to program source code | Access to program source code shall be restricted. | Digital Realty SOC 2 control does not map back to this control. |

### A.10.1 – Cryptographic Controls

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.10.1.1 | Policy on the use of cryptographic controls | A policy on the use of cryptographic controls for protection of information shall be developed and implemented. | Digital Realty SOC 2 control does not map back to this control. |
| A.10.1.2 | Key management | A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle. | Digital Realty SOC 2 control does not map back to this control. |

### A.11.1 – Secure Areas

To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.11.1.1 | Physical security perimeter | Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information process facilities. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| A.11.1.2 | Physical entry controls | Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | | | CC6.4.2: Physical access requests are documented and require the approval of the relevant access authorizer. |
| A.11.1.3 | Securing offices, rooms, and facilities | Physical security for offices, rooms and facilities shall be designed and applied. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| A.11.1.4 | Protecting against external and environmental threats | Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| A.11.1.5 | Working in secure areas | Procedures for working in secure areas shall be designed and applied. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| A.11.1.6 | Delivery and loading areas | Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |

**A.11.2 – Equipment**

To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.11.2.1 | Equipment siting and protection | Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. | CC6.4.1: Physical access controls are in place to restrict access to and within the data center facilities. |
| | | | A1.2.3: The data centers are equipped with the following environmental protection equipment:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |
| | | | A1.2.4: Management retains the inspection report received from third party specialists evidencing completion of inspection and maintenance of the following according to a predefined schedule:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |
| | | | A1.2.5: Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring. |
| | | | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| A.11.2.2 | Supporting utilities | Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| | | | A1.2.3: The data centers are equipped with the following environmental protection equipment:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| | | | A1.2.4: Management retains the inspection report received from third party specialists evidencing completion of inspection and maintenance of the following on at least an annual basis:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |
| | | | A1.2.5: Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring. |
| A.11.2.3 | Cabling security | Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage. | A1.2.3: The data centers are equipped with the following environmental protection equipment:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |
| A.11.2.4 | Equipment maintenance | Equipment shall be correctly maintained to ensure its continued availability and integrity. | A1.2.4: Management retains the inspection report received from third party specialists evidencing completion of inspection and maintenance of the following on at least an annual basis:<br>· Fire detection and suppression equipment<br>· UPS systems<br>· Generators<br>· HVAC Systems |
| A.11.2.5 | Removal of assets | Equipment, information, or software shall not be taken off-site without prior authorization. | Digital Realty SOC 2 control does not map back to this control. |
| A.11.2.6 | Security of equipment and assets off-premises | Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises. | Digital Realty SOC 2 control does not map back to this control. |
| A.11.2.7 | Secure disposal or re-use of equipment | All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. | CC6.5.1: Documented media sanitation policies are in place to guide personnel in the disposal of confidential information stored on media devices. |
| | | | CC6.5.2: Requests to dispose of media devices containing confidential information are entered via the ticketing system and disposed. Customers receive a receipt of data destruction upon completion of data disposal. |
| A.11.2.8 | Unattended user equipment | Users shall ensure that unattended equipment has appropriate protection. | Digital Realty SOC 2 control does not map back to this control. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.11.2.9 | Clear desk and clear screen policy | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. | Digital Realty SOC 2 control does not map back to this control. |

### A.12.1 – Operational Procedures and Responsibilities

To ensure correct and secure operations of information processing facilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.1.1 | Documented operating procedures | Operating procedures shall be documented and made available to all users who need them. | A1.2.5: Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring. |
| | | | CC1.1.3: Policies and procedures require that employees sign an acknowledgment form upon hire indicating that they have been given access to the employee policies and procedures and understand their responsibility for adhering to the code of conduct outlined within the policies and procedures. |
| | | | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| | | | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| | | | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| A.12.1.2 | Change management | Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled. | CC8.1.1: Documented policies and procedures are in place to guide personnel in the release management and change management process. |
| | | | CC8.1.2: A change management meeting is held on a monthly basis to discuss and communicate the past, ongoing, and upcoming projects that affect the system. |
| | | | CC8.1.3: Changes to network devices are logged, tested where applicable, approved, and closed in a timely manner. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| | | | CC8.1.4: Requests for changes, system maintenance, and supplier maintenance are documented, prioritized, tested, and approved. |
| A.12.1.3 | Capacity management | The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. | A1.1.1 & A1.2.1: BMS applications are configured to monitor environmental systems and alert the facility team when predefined thresholds have been met. |
| | | | A1.1.2: Management meetings are held on at least a quarterly basis to review availability trends and availability forecasts as compared to system requirements. |
| A.12.1.4 | Separation of development, testing and operational environments | Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment. | Digital Realty SOC 2 control does not map back to this control. |

### A.12.2 – Protection from Malware

To ensure that information and information processing facilities are protected against malware.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.2.1 | Controls against malware | Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. | CC2.1.2, CC4.1.3, CC4.2.3, CC6.8.1, CC7.1.4, & CC7.2.4: A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. |
| | | | CC4.1.4, CC4.2.4, CC6.8.2, CC7.1.2, & CC7.2.2: An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. |

### A.12.3 – Backup

To protect against loss of data.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.3.1 | Information backup | Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. | Digital Realty SOC 2 control does not map back to this control. |

### A.12.4 – Logging and Monitoring

To record events and generate evidence.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.4.1 | Event logging | Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed. | CC4.1.4, CC4.2.4, CC6.8.2, CC7.1.2, & CC7.2.2: An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. |
| A.12.4.2 | Protection of log information | Logging facilities and log information shall be protected against tampering and unauthorized access. | CC6.1.3 & CC6.3.3: Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. |
| A.12.4.3 | Administrator and operator logs | System administrator and system operator activities shall be logged, and the logs protected and regularly reviewed. | CC4.1.4, CC4.2.4, CC6.8.2, CC7.1.2, & CC7.2.2: An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. |
| A.12.4.4 | Clock synchronization | The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source. | Digital Realty SOC 2 control does not map back to this control. |

### A.12.5 – Control of Operational Software

To ensure the integrity of operational systems.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.5.1 | Installation of software on operational systems | Procedures shall be implemented to control the installation of software on operational systems. | Digital Realty SOC 2 control does not map back to this control. |

### A.12.6 – Technical Vulnerability Management

To prevent exploitation of technical vulnerabilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.6.1 | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | CC2.1.2, CC4.1.3, CC4.2.3, CC6.8.1, CC7.1.4, & CC7.2.4: A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. |
| | | | CC2.1.3: Security management systems are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. |
| | | | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| | | | CC4.1.5 & CC4.2.5: External assessments are conducted by an accredited independent third-party assessor on an annual basis. The results of the audits are reviewed by management as part of the management review process. |
| | | | CC9.2.3: Management performs service reviews of third-party vendors on an at least an annual basis to help ensure that third party vendors maintain compliance with security and availability commitments. |
| A.12.6.2 | Restrictions of software installation | Rules governing the installation of software by users shall be established and implemented. | Digital Realty SOC 2 control does not map back to this control. |

### A.12.7 – Information Systems Audit Considerations

To minimize the impact of audit activities on operational systems.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.12.7.1 | Information systems audit controls | Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes. | CC2.1.6, CC2.2.6, CC2.3.3, & CC4.2.6: Annual assessments are performed by the compliance team. These assessments include evaluation of the operation of key controls. Assessments are reviewed and require the development of corrective action plans for control weaknesses. |

### A.13.1 – Network Security Management

To ensure the protection of information in networks and its supporting information processing facilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.13.1.1 | Network controls | Networks shall be managed and controlled to protect information in systems and applications. | CC4.1.4, CC4.2.4, CC6.8.2, CC7.1.2, & CC7.2.2: An IDS is deployed throughout the environment to monitor and prevent malicious activity at the log and network levels. IT personnel are alerted of events via e-mail notification. |
| A.13.1.2 | Security of network services | Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| A.13.1.3 | Segregation in networks | Groups of information services, users and information systems shall be segregated on networks. | CC6.1.3 & CC6.3.3: Predefined security groups are utilized to assign least privilege based access privileges and segregate access to data to the in-scope systems. |

### A.13.2 – Information Transfer

To maintain the security of information transferred within an organization and with any external entity.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.13.2.1 | Information transfer policies and procedures | Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. | Digital Realty SOC 2 control does not map back to this control. |
| A.13.2.2 | Agreements on information transfer | Agreements shall address the secure transfer of business information between the organization and external parties. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| A.13.2.3 | Electronic messaging | Information involved in electronic messaging shall be appropriately protected. | Digital Realty SOC 2 control does not map back to this control. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.13.2.4 | Confidentiality or non-disclosure agreements | Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |

### A.14.1 – Security Requirements of Information Systems

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.14.1.1 | Information security requirements analysis and specification | The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.1.2 | Securing application services on public networks | Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.1.3 | Protecting application services transactions | Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | Digital Realty SOC 2 control does not map back to this control. |

### A.14.2 – Security in Development and Support Processes

To ensure that information security is designed and implemented within the development lifecycle of information systems.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.14.2.1 | Secure development policy | Rules for the development of software and systems shall be established and applied to developments within the organization. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.2.2 | System change control procedures | Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.2.3 | Technical review of applications after operating platform changes | When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | Digital Realty SOC 2 control does not map back to this control. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.14.2.4 | Restrictions on changes to software packages | Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.2.5 | Secure system engineering principles | Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.2.6 | Secure development environment | Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.2.7 | Outsourced development | The organization shall supervise and monitor the activity of outsourced system development. | Digital Realty SOC 2 control does not map back to this control. |
| A.14.2.8 | System security testing | Testing of security functionality shall be carried out during development. | CC8.1.3: Changes to network devices are logged, tested where applicable, approved, and closed in a timely manner. |
| | | | CC8.1.4: Requests for changes, system maintenance, and supplier maintenance are documented, prioritized, tested, and approved. |
| A.14.2.9 | System acceptance testing | Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new versions. | CC8.1.3: Changes to network devices are logged, tested where applicable, approved, and closed in a timely manner. |
| | | | CC8.1.4: Requests for changes, system maintenance, and supplier maintenance are documented, prioritized, tested, and approved. |

**A.14.3 – Test Data**

To ensure the protection of data used for testing.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.14.3.1 | Protection of test data | Test data shall be selected carefully, protected, and controlled. | Digital Realty SOC 2 control does not map back to this control. |

### A.15.1 – Information Security in Supplier Relationships

To ensure protection of the organization's assets that is accessible by suppliers.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.15.1.1 | Information security policy for supplier relationships | Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. | CC1.1.4, CC2.1.5, CC2.2.1, & CC6.1.1: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company Intranet. |
| | | | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| | | | CC9.2.1: A vendor management policy is in place that addresses specific requirements for a vendor and the supporting monitoring and review process. |
| | | | CC9.2.2: The entity's established vendor requirements, scope of services, roles, and responsibilities and service levels are documented in vendor contracts. |
| A.15.1.2 | Addressing security within supplier agreements | All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| | | | CC9.2.1: A vendor management policy is in place that addresses specific requirements for a vendor and the supporting monitoring and review process. |
| | | | CC9.2.2: The entity's established vendor requirements, scope of services, roles, and responsibilities and service levels are documented in vendor contracts. |
| A.15.1.3 | Information and communication technology supply chain | Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |

### A.15.2 – Supplier Service Delivery Management

To maintain an agreed level of information security and service delivery in line with supplier agreements.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.15.2.1 | Monitoring and review of supplier services | Organizations shall regularly monitor, review and audit supplier service delivery. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| | | | CC9.2.3: Management performs service reviews of third-party vendors on an at least an annual basis to help ensure that third party vendors maintain compliance with security and availability commitments. |
| A.15.2.2 | Managing changes to supplier services | Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| | | | CC9.2.3: Management performs service reviews of third-party vendors on an at least an annual basis to help ensure that third party vendors maintain compliance with security and availability commitments. |

### A.16.1 – Management of Information Security Incidents and Improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.16.1.1 | Responsibilities and procedures | Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.16.1.2 | Reporting information security events | Information security events shall be reported through appropriate management channels as quickly as possible. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| A.16.1.3 | Reporting information security weaknesses | Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| A.16.1.4 | Assessment of and decision on information security events | Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.16.1.5 | Response to information security incidents | Information security incidents shall be responded to in accordance with the documented procedures. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |
| A.16.1.6 | Learning from information security incidents | Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| A.16.1.7 | Collection of evidence | The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence. | CC2.1.1, CC3.2.4, CC4.1.2, CC4.2.2, CC7.3.1, CC7.4.4, & CC7.5.3: Management meetings are held on at least a monthly basis to discuss the effect of identified security and availability vulnerabilities on the ability to meet business objectives and commitments and to identify corrective measures. |
| | | | CC2.2.5, CC2.3.2, CC4.1.1, CC4.2.1, CC7.1.1, CC7.2.1, & CC7.4.1: Documented escalation procedures for reporting security and availability incidents are provided to internal and external users to guide users in identifying, reporting, and remediating failures, incidents, concerns, and other complaints. |

### A.17.1 – Information Security Continuity

Information security continuity shall be embedded in the organization's business continuity management systems.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.17.1.1 | Planning information security continuity | The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.17.1.2 | Implementing information security continuity | The organization shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |
| A.17.1.3 | Verify, review, and evaluate information security continuity | The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |

### A.17.2 – Redundancies

To ensure availability of information processing facilities.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.17.2.1 | Availability of information processing facilities | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. | CC9.1.2, A1.2.2, & A1.3.1: Emergency recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. |

### A.18.1 – Compliance with Legal and Contractual Requirements

To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.18.1.1 | Identification of applicable legislation and contractual requirements | All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organization. | CC2.1.7 & CC3.4.1: The IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. |
| | | | CC2.3.1: The entity's security and availability commitments and the associated system requirements are documented in customer agreements to include relevant service level and nondisclosure terms. |
| | | | CC2.3.5: The director of site operations performs an annual review of the Digital Realty security post orders including system security changes that might impact local property teams. The approved post orders are disseminated to the local site management by site operations |
| | | | CC8.1.2: A change management meeting is held on a monthly basis to discuss and communicate the past, ongoing, and upcoming projects that affect the system. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.18.1.2 | Intellectual property rights | Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products. | CC2.1.7 & CC3.4.1: The IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. |
| A.18.1.3 | Protection of records | Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislatory, regulatory, contractual, and business requirements. | CC2.1.7 & CC3.4.1: The IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. |
| A.18.1.4 | Privacy and protection of personally identifiable information | Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable. | Digital Realty SOC 2 control does not map back to this control. |
| A.18.1.5 | Regulation of cryptographic controls | Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations. | Digital Realty SOC 2 control does not map back to this control. |

**A.18.2 – Information Security Reviews**

To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| A.18.2.1 | Independent review of information security | The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur. | CC2.1.2, CC4.1.3, CC4.2.3, CC6.8.1, CC7.1.4, & CC7.2.4: A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. |
| | | | CC2.1.3: Security management systems are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. |
| | | | CC9.2.3: Management performs service reviews of third-party vendors on an at least an annual basis to help ensure that third party vendors maintain compliance with security and availability commitments. |
| A.18.2.2 | Compliance with security policies and standards | Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements. | CC1.1.5: Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures. |
| | | | CC1.3.1: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed. |

| ISO # | ISO Description | ISO Control Activity | Related Digital Realty Controls |
|---|---|---|---|
| | | | CC1.3.3: Management assigns the responsibility of the maintenance and enforcement of the entity security and availability policies and procedures to the compliance team. |
| | | | CC1.4.4 & CC2.2.3: Management monitors compliance with training requirements on an annual basis. |
| | | | CC2.1.6, CC2.2.6, CC2.3.3, & CC4.2.6: Annual assessments are performed by the compliance team. These assessments include evaluation of the operation of key controls. Assessments are reviewed and require the development of corrective action plans for control weaknesses. |
| A.18.2.3 | Technical compliance review | Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards. | CC3.1.3, CC3.2.2, & CC3.4.3: Technical operations perform a risk assessment on an annual basis to identify and analyze the business and security risks, vulnerabilities, laws, and regulations. The risk assessment also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats, and vulnerabilities arising from business partners, customers, and others with access to the entity's information system. Risks identified are formally documented, analyzed for their significance, and reviewed by management, along with mitigation strategies. |
| | | | CC2.1.2, CC4.1.3, CC4.2.3, CC6.8.1, CC7.1.4, & CC7.2.4: A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal policy SLAs. |
| | | | CC2.1.3: Security management systems are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. |