EQUINIX

SOC 2 REPORT

FOR

DATA CENTER HOSTING SERVICES

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

NOVEMBER 1, 2018, TO OCTOBER 31, 2019

Attestation and Compliance Services

Proprietary & Confidential
Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

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

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

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

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Equinix, Inc:

Scope

We have examined Equinix, Inc.'s ("Equinix" or the "service organization") accompanying description of its Data Center Hosting Services system, in Section 3, throughout the period November 1, 2018, to October 31, 2019, (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 November 1, 2018, to October 31, 2019, to provide reasonable assurance that Equinix's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Equinix uses a subservice organization for all of the environmental protection controls at the Chicago 4 (CH4) data center facility and all of the physical security controls at the Dallas 10 (DA10) data center facility. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Equinix, to achieve Equinix's service commitments and system requirements based on the applicable trust services criteria. The description presents Equinix's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Equinix's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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.

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

As indicated in the accompanying description of the system, Equinix sold the New York 12 (NY12) data center facility on October 11, 2019. Therefore, any references to controls at the NY12 data center are specific to the facility's dates of operation under Equinix ownership, and during the period November 1, 2018, to October 11, 2019.

In our opinion, in all material respects,

a. the description presents Equinix's Data Center Hosting Services system that was designed and implemented throughout the period November 1, 2018, to October 11, 2019 for the NY12 data center facility, and November 1, 2018, to October 31, 2019 for all other in scope data center facilities described in Section 3 below, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period November 1, 2018, to October 11, 2019 for the NY12 data center facility, and November 1, 2018, to October 31, 2019 for all other in scope data center facilities described in Section 3 below, to provide reasonable assurance that Equinix's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Equinix's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period November 1, 2018, to October 11, 2019 for the NY12 data center facility, and November 1, 2018, to October 31, 2019 for all other in scope data center facilities described in Section 3 below, to provide reasonable assurance that Equinix's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Equinix's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Equinix; user entities of Equinix's Data Center Hosting Services system during some or all of the period November 1, 2018, to October 31, 2019, business partners of Equinix subject to risks arising from interactions with the Data Center Hosting 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;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

Schellman & Company, LLC

Tampa, Florida
December 6,2019

SECTION 2

MANAGEMENT'S ASSERTION

EQUINIX

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Equinix's Data Center Hosting Services system, in Section 3, throughout the period November 1, 2018, to October 31, 2019, (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 Hosting Services system that may be useful when assessing the risks arising from interactions with Equinix's system, particularly information about system controls that Equinix 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)*.

Equinix uses a subservice organization for all of the environmental protection controls at the Chicago 4 (CH4) data center facility and all of the physical security controls at the Dallas 10 (DA10) data center facility. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Equinix, to achieve Equinix's service commitments and system requirements based on the applicable trust services criteria. The description presents Equinix's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Equinix's controls. The description does not disclose the actual controls at the subservice organization.

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

a. the description presents Equinix's Data Center Hosting Services system that was designed and implemented throughout the period November 1, 2018, to October 31, 2019, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period November 1, 2018, to October 31, 2019, to provide reasonable assurance that Equinix's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Equinix's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period November 1, 2018, to October 31, 2019, to provide reasonable assurance that Equinix's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Equinix's controls operated effectively throughout that period.

As indicated in our description of the system, the New York 12 (NY12) data center facility was sold on October 11, 2019. Therefore, any references to controls at the NY12 data center facility are specific to the facility's dates of operation under Equinix ownership, and during the period November 1, 2018, to October 11, 2019.

Section 3

Description of the System

Overview of Operations

Company Background

Equinix was founded in 1998 and operates International Business Exchange™ (IBX) data centers offering businesses a place to run their operations and exchange information. Equinix's interconnection platform spans 53 markets on five continents and hosts a comprehensive portfolio of digital services and ecosystems that allows customers to securely scale their digital infrastructure wherever opportunity leads. More than 9,800 companies populate Equinix's diverse ecosystems, and all are potential partners or customers.

Description of Services Provided

Equinix provides data center hosting services at its Americas IBX data center facilities identified in the System Boundaries section below. The sites offer reliability, redundancy, and customization to meet the unique business needs of a wide range of customers spanning across numerous industry verticals. Equinix's data center hosting services includes the physical infrastructure, power, and data connectivity for its customer's information systems. It also includes the implementation, maintenance, and administration of physical access control systems for the safeguard customer information systems and assets, and environmental protection systems to reduce the risk of environmental threats (i.e. power loss, fire, flooding).

Principal Service Commitments and System Requirements

Equinix designs its processes and procedures related to the system to meet its objectives for its data center hosting services. Those objectives are based on the service commitments that Equinix makes to user entities, the laws and regulations that govern the provision of the data center hosting services, and the financial, operational, and compliance requirements that Equinix has established for the services. The data center hosting services of Equinix are subject to the relevant regulatory and industry information and data security requirements in which Equinix operates.

Security and availability commitments to user entities are documented and communicated in service agreements and other customer agreements, sales and marketing documentation, as well as in the description of the service offering provided online. The principal security and availability commitments are standardized and include, but are not limited to, the following:

- Implementing and maintaining security systems and controls at its IBX data centers and facilities to protect the confidentiality, integrity, and availability of customer's mission critical information technology (IT) equipment and information; including the establishment of safeguards to protect information resources against, theft, abuse, misuse, distortion, or any form of illegal damage.
- Providing reliable and highly-available IBX data center environments through the maintenance and continuous monitoring of environmental conditions and systems for adherence to Equinix's availability service-level commitments, including the following:
    - Temperature levels controlled between 64.4°F (18°C) and 80.6°F (27°C)
    - Relative humidity levels controlled between 25% and 65%
    - 99.999%+ redundant and 99.99%+ non-redundant power availability
- Establishing and sustaining incident response, disaster recovery and business continuity programs to respond to and recover from incidents or major service interruptions in a timely manner with minimal damage to customer and company assets, and impact to the services provided.
- Ensuring Equinix's compliance with the applicable legal, statutory, regulatory requirements, including relevant country-specific regulations.

Equinix establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. This includes defined company policies and procedures focused on reducing risks related to the achievement of objectives for security and availability; and the implementation of a company-wide systematic approach for performing annual risk assessments to identify threats and vulnerabilities to objectives and the application of the risk treatment activities to mitigate said risks. It also includes screening procedures during the hiring process; administration of annual formal security awareness training program completion requirements for all personnel; and the use of preventative, detective and responsive control processes and mechanisms to ensure physical and logical access to information and systems is restricted to authorized individuals, as well as to ensure facilities housing customer equipment and support operations are properly provisioned, maintained and monitored to reduce the risks of environmental threats such as power loss, fire, and flooding.

Such requirements are communicated in Equinix's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Data Center Hosting Services system.

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

Components of the System Used to Provide the Service

System Boundaries

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

The scope of the review includes the Data Center Hosting Services performed at the data center facilities located in the metropolitan areas listed below. Additionally, the support and management functions of the Tampa, Florida, field office (TPFO) relevant to the Data Center Hosting Services were included within the scope of the review.

[Intentionally Blank]

Specifically, the following sites were included within the scope of the review:

Tampa, Florida
- TPFO

Silicon Valley, California
- SV1
- SV2
- SV3
- SV4
- SV5
- SV6
- SV8
- SV10
- SV13
- SV14
- SV15
- SV16
- SV17

Los Angeles, California
- LA1
- LA2
- LA3
- LA4
- LA7

Atlanta, Georgia
- AT1
- AT2
- AT3
- AT4
- AT5

Washington, D.C.
- DC1
- DC2
- DC3
- DC4
- DC5
- DC6
- DC7
- DC8
- DC10
- DC11
- DC12
- DC13
- DC14
- DC97

Toronto, Ontario
- TR1
- TR2

Seattle, Washington
- SE2
- SE3
- SE4

Houston, Texas
- HO1

Boston, Massachusetts
- BO1
- BO2

Dallas, Texas
- DA1
- DA2
- DA3
- DA4
- DA6
- DA7
- DA9
- DA10 (environmental only)

Chicago, Illinois
- CH1
- CH2
- CH3
- CH4 (physical only)
- CH7

Culpeper, Virginia
- CU1
- CU2
- CU3
- CU4

Philadelphia, Pennsylvania
- PH1

Miami, Florida
- MI1
- MI2
- MI3
- MI6

Denver, Colorado
- DE1
- DE2

New York, New York
- NY1
- NY2
- NY4
- NY5
- NY6
- NY7
- NY8
- NY9
- NY11
- NY12 (former)*
- NY13

São Paulo, Brazil
- SP1
- SP2
- SP3
- SP4

Rio De Janeiro, Brazil
- RJ1
- RJ2

Bogotá, Colombia
- BG1

*Equinix no longer owns the New York 12 (NY12) data center facility, after completing its sale to Verizon Communications, Inc. (Verizon) on October 11, 2019, at which time NY12 site operations were fully turned over to Verizon.

Infrastructure and Software

Equinix's Data Center Hosting Services system comprises the physical infrastructure, power, and data connectivity needed to house customer information systems, assets, and data at its IBX facilities; and includes the provision of physical and environmental security mechanisms to safeguard those customer assets from unauthorized access and environmental threats.

A combination of custom developed, externally supported, and wholly purchased application platforms are utilized to support the delivery data center services. The applications are housed on Dell servers and virtual machines (VMs) running Microsoft Windows and Red Hat Enterprise Linux operating systems.

The following table provides a summary of the in-scope infrastructure and information systems:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System**	**Physical Location**
Physical access control systems (various platforms – varies by region / location)	Biometric, proximity card, and/or personal identification number (PIN) reader system (varies by data center facility) used to restrict data center access to only those individuals provisioned with access; the systems are also used to monitor, log, and notify personnel of physical security alarms	Windows / Linux	Data center facilities / Equinix Operations Center (EOC)
Closed circuit television (CCTV) system (various platforms – varies by region / location)	Surveillance camera system used for security monitoring of data centers 24 hours per day; CCTV cameras are positioned throughout the data centers to monitor and track the activity of any person while inside and outside of the data centers	Windows / Linux	Data center facilities / EOC
Building Management System (BMS) (various platforms – varies by region / location)	Building management system used to monitor environmental controls and alert data center personnel to potential issues within the data center, including critical electrical components, power management equipment, heating, ventilation, and air-conditioning (HVAC) equipment, and fire detection and suppression equipment	Windows / Linux	Data center facilities / EOC
Equinix Customer Portal (ECP)	Web-based portal used by customers to manage their access control lists including access change requests and visitor access requests to data center; place orders for IBX data center products and schedule services; and view order statuses, access reports, account information, and review invoices	Windows / Linux	Corporate IT / Network Operations Center (NOC)
Global Service Desk (GSD) and Siebel ticketing systems	Ticketing system used to record, track, and monitor internal and external reported incidents, requests, and notifications applicable to physical and environmental security matters	Windows / Linux	Data center facilities / EOC
IBM Maximo	Enterprise asset management system used to inventory and track assets for the IBX data center, as well as to schedule preventive and predictive maintenance work visits, issue work ticket, track costs, and records maintenance history	Windows / Linux	Data center facilities / EOC
Microsoft Active Directory (AD)	Directory services used to manage user accounts, access, and authentication requirements	Windows	Corporate IT / NOC
Firewalls, VPN gateways, routers, and switches	Corporate IT managed network devices and systems utilized to restrict, filter, and route traffic for Equinix's corporate network; VPN gateways Network devices used to facilitate secure connectivity to the Equinix corporate for data centers (site-to-site) and end users (point-to-point)	Palo Alto / Juniper / Cisco / Opengear / Avocent	Corporate IT / NOC

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System**	**Physical Location**
File storage systems	Disk storage devices used to present files and directories to local host and to hosts over the network	Windows / Linux	Corporate IT / NOC / Data center facilities

As noted in the 'Subservice Organizations' section below, the physical access control systems for DA10, and environmental control systems for CH4 are hosted on infrastructure owned by Digital Realty Trust, Inc. (Digital Realty Trust). The Data Center Hosting Services system is limited to the services and related infrastructure maintained by Equinix and does not include Digital Realty Trust, user entity systems, or the Internet connectivity utilized for accessing user entity environments.

People

Equinix has data centers across North and South America that are manned with employees to support security and reliability to Equinix's customers. The majority of other functions, including IT, finance, legal, marketing, operations, sales, and other administrative functions are centralized at the corporate level, though some of the staff and management work from remote locations.

As Equinix grows over time, positions are added to provide additional management guidance, oversight, and structure. Organizational directory structures are available on Equinix's intranet and are updated frequently for new hires, promotions, or departures. Lines of authority are clearly defined and communicated within the organization.

Equinix's internal leadership focuses on finding new ways to bring innovation, leadership, and quality to support the company's objective to be the interconnection platform for the world's leading businesses. Executive and regional management teams meet regularly to discuss such topics as emerging trends, potential risks to the organization, and potential new strategies. These teams are composed of a cross functional group of executives to prevent domination by only one or two individuals. The global executive team includes the president and chief executive officer; executive vice president, global operations; chief product officer; chief sales officer; chief technology officer; chief legal and human resources officer; chief strategy and development officer; chief customer and revenue officer; chief financial officer; executive chairman; and senior vice president, chief information officer. Regional managements teams comprised a president, senior vice president of sales, and managing director(s) are in place to oversee the management, strategy, and growth of Equinix in the Americas; Europe, Middle East, and Africa (EMEA); and Asia-Pacific (AP).

Each year, the executive team meets for a formal business strategy and planning exercise. These topics are communicated to Equinix employees through all-hands meetings, which are held at least annually, by the executive team.

Procedures

Physical Security

IBX Infrastructure

Each IBX data center utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. Exterior walls may incorporate additional security measures, such as reinforced concrete, Kevlar bullet board, vapor barriers, or bullet-resistant front doors. Colocation and IBX floor areas have window-less exteriors. In case due to the existing infrastructure there are windows leading to the exterior then they need to be locked from the inside or access controlled. In many of the IBXs, exterior perimeter walls, doors, and windows, and the main interior entry door to the colocation floor, are constructed of materials that afford Underwriters Laboratories, Inc. rated ballistic protection.

All areas of the data center, including cages, are monitored and recorded using CCTV, and access points are controlled. The CCTV subsystem provides the display, control, digital recording, and playback of live video from cameras throughout the facility. This system is integrated with the alarm monitoring/intrusion detection subsystem, so in the event of an alarm condition, cameras may be called up to record the area where the alarm condition is occurring. Each camera is capable of accelerating digital recording during alarm conditions for better resolution. The alarm monitoring/intrusion detection subsystem monitors the status of various devices associated with the security system, such as alarm contacts, glass breakage detectors, motion detectors, and tamper switches. If the status of any of these devices changes from their secure state, an alarm will be activated and displayed on the security system workstation and recorded on the system server's hard drive.

The IBX data centers are staffed on a 24-hour basis by a professional security staff or operations team, which monitors access points and monitors the electronic security systems. At each IBX, where there is a minimum of two security officers, at least one officer needs to be present to man the security kiosk and any additional officers may perform security walk throughs of the IBX. Doors, including cages, are secured with biometric hand geometry readers or proximity card readers. For shared cages, there are kinetic locks on the cabinets. Security systems have dedicated uninterruptible power supply (UPS) systems and standby emergency power (generator) support.

Other security features and controls may include:

- Control points between exterior and customer equipment
- 90-day video activity storage, and at minimum 30 days
- Weekly cross-IBX security meetings
- Customer self-administration of authority levels for ordering and access
- Segregation of order management (done by customer service and/or sales) and service delivery functions in order to assure no "local agreements"
- Customer privacy policies, including no pictures and customer anonymity
- Facility design, which includes controlled access points, reinforced exterior walls
- Token authentication required for access to enterprise network
- Bullet-resistant protection
- Motion-detection lighting, and automatic lighting that activated in the event of a power outage or disruption including facility emergency exits

Ingress mantraps are in place and administered to help restrict access to IBX facilities to only authorized individuals. The IBX design specifications for the "mantrap" door interlocks mandate that no two adjacent doors may be open at the same time (e.g. the door into the lobby from the outside and the door into the mantrap may not be open at the same time; another example, the door into the mantrap and the door out of the mantrap may not be open at the same time). This is to prevent anyone from bypassing in-place security access procedures (both system and officer driven) when entering or exiting the IBX site.

Equinix uses biometric hand scanners, proximity card readers or a combination thereof to allow authorized users access into the building and through various doors within the facility. Through a combination of hand scan and numeric code or a valid proximity card, users identify themselves to the system and obtain access into certain areas of the IBX based upon the predefined user permissions. Biometric scanners are not required on the collocation side of doors to exit the collocation area into the customer care/common areas. Entry to customer cages from the exterior of the IBX requires access from a minimum of four to five biometric scanners or badge access readers. Cage security is provided through multiple levels of access control: hand geometry readers at the cage entrance, keyed locks at each cage, and if the cabinet is located in a shared-cage environment, the cabinet door includes a self-powered, keypad-activated lock. The lock permits up to 99 authorized entrants. Access histories can be downloaded by Equinix personnel and are available to the customer for auditing purposes through Smart Hands. In some areas inside the IBX that are under Equinix control (e.g. battery rooms), proxy card readers are used instead of biometrics for convenience of Equinix personnel.

The LA2 IBX facility was not constructed by Equinix. Size constraints limited the amount of remodeling that could be accomplished, and exceptions were allowed in the redesign. The LA2 facility has one biometric hand scan reader located at the entrance to the site. Instead of a mantrap, security officers electronically unlock the door to the colocation floor once they have verified the customer's identification (ID) and validated their visit. In place of hand scan readers on every cage door, physical keys are provided to customers of this site that are used to access their cages.

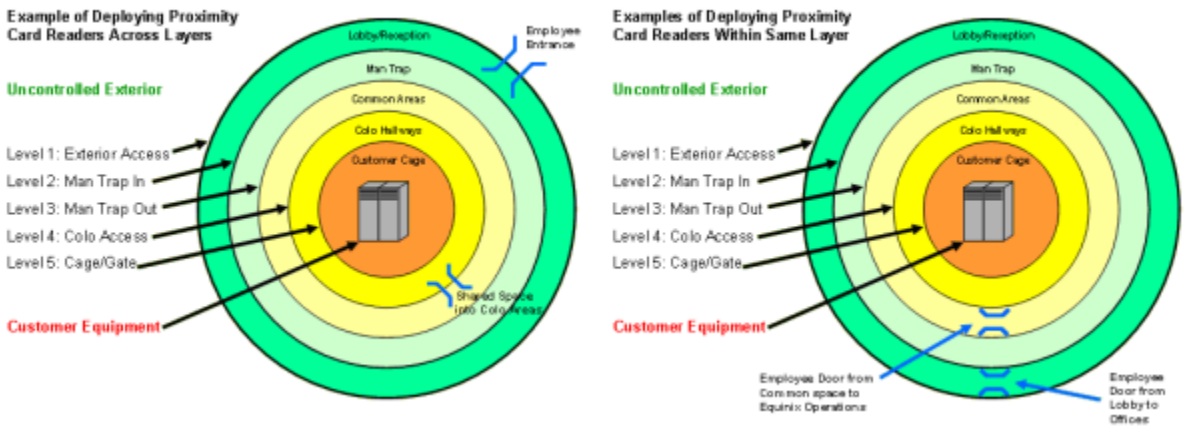
Employee Data Center Access

Equinix has documentation in place to outline the requirements related to restricting and controlling access to IBX facilities. The main goal of these security procedures and protocols is the protection of people and of assets belonging to Equinix and its customers. Assets are defined as both property and information. Employees are provided access to the specific IBX locations where they perform their job duties. A Service Request (SR) is created by the GSD upon a request by the hiring manager. It is Equinix company policy to issue ID badges to each Equinix employee and to temporary agency and contractor personnel. These policies apply to employees, trainees, temporary agency workers, and Equinix contractor personnel.

The Siebel ticketing system is a web-based portal that security personnel use to view requests for access, access enrollment authorization, and removal, etc. The data written into the log and notes section of a SR is used to update the status of the SR. Proximity card issuance and biometric profile setup and modification activities are performed by security personnel only upon receipt of an access enrollment requests ticket, which indicates the person is an authorized Equinix employee or contractor.

Personnel authorized to work at an Equinix facility are required to display ID badges when entering or working within an Equinix IBX. Depending on the access privileges, off-site employees may be required to be escorted by authorized personnel while within the facility.

Proximity card readers are installed on doors/gates, which provide access to areas restricted to Equinix employees and/or authorized contractors and do not cross boundaries or security layers established to protect customer equipment. Readers equipped with numeric keypads will be utilized on card reader doors, which cross a boundary between areas or layers of security separated by biometric hand scan readers. Long-range proximity readers are installed at vehicle access gates at some of the IBX locations, which control access to areas surrounding shipping/receiving doors and/or loading docks.



Temporary use badges are issued by security personnel only upon receipt of written or electronic authorization from Equinix management. A temporary use badge may be issued to an employee in the case their badge is lost or if the employee forgets to bring it to work. Security officers check a government-issued photo ID to verify the identity of persons requesting a sign-out badge. The person checking out the badge is required to return the badge after use when exiting the facility. Issuance of sign-out badges is also documented within an access security form. Security personnel notify Equinix management if any badge is not returned within 24 hours of issuance.

Customer Data Center Access

Customers are required to sign a contract and a nondisclosure agreement with Equinix. Customers submit their access requests either through the ECP or the GSD. Authorized customers are provided a unique identifier and password and granted access via specific roles within the Siebel ticketing system. Siebel is the primary database used for maintaining customer contacts and their physical access permissions.

Customer administrators can assign physical access to authorized personnel who have a business purpose and need to gain physical access to an IBX data center. This individual(s) can be an employee or contractor of the customer. All enrollees must present a government-issued photo ID to security upon arrival to complete the Access Enrollment process to create a biometric and proximity card reader access account in the IBX access control system. Only customers with IBX access services permission are allowed to place Work Visits and Tours orders through ECP or GSD after verification. Work visits and tour activities are created in Siebel. The security guards set up the access based on the work visits or tours activities noted within Siebel. Customers accessing the IBX facility are required to display ID badges when entering an Equinix IBX facility.

Certain IBX data centers utilize the “Fast Pass” photo ID program, which serves as an alternative form of identification for customers who visit an IBX facility frequently. The IBX data center managers or their designees are responsible for determining who may be issued a Fast Pass and approving the Fast Pass users. Qualified Fast Pass users are issued either local or national Fast Pass IDs, which are used instead of their government ID. Holding a Fast Pass ID eliminates a number of check-in procedures for the user and expedites their entrance. Fast Pass holders do not need to wait for a sticker badge to be printed, and site security will log their entry for them.

Vendor and Contractor Data Center Access

Vendors and contractors follow access procedures similar to those of customers. For an Equinix contractor, a work visit ticket will be created by an employee and the contractor is required to be escorted and is monitored on cameras. In some cases, long-term Equinix contractors are allowed unescorted access to open areas but not to customer cages. If they need to work within a cage, they are escorted by Equinix personnel or security.

Visitor Data Center Access

Visitors are screened upon entry to verify their identity. The security guard checks the government issued photo ID, and visitors are required to sign in.

Physical Access Removal

Biometric and proximity card reader access to the IBX-secured areas is removed upon receipt of customer request by security. Access removals are a high priority and must be acted upon within two hours of receiving the notification in Siebel. In order to help ensure tracking and customer notification, the security officer records the completion of access removal activities within a Siebel ticket. ID cards associated with the user are also canceled. In order to maintain accurate history records, individuals are never deleted from an access list and are moved from an active to an inactive status.

ID badge and proximity cards for site staff are surrendered to supervisors or an Equinix point of contact immediately upon termination of employment or upon request from Equinix management.

Security Personnel Formal Training

All security officers are required to complete mandatory security training prior to their full-time assignment at Equinix. Security personnel formal training includes security-specific training that third-party security service provider administers to its officers, as well as Equinix specific training once they are assigned to Equinix. The training comprises a five-day schedule. A summary of the training includes the following:

- Equinix company overview
- Safety training videos and/or classes
- Walkthrough of the IBX and orientation of the various equipment
- Security officer responsibilities, including assigning access and access enrollment procedures

- Security systems walkthrough of access control
- Response to emergencies, including fire alarms, bomb threats, and other natural disasters and evacuation procedures
- Incident reporting
- Site-specific procedures

A checklist record is maintained of the completed training and both the trainer and trainee sign a checklist acknowledging the completion of the training. In addition to the checklist, the trainer administers an exam at the end of 16 hours and a final exam at the end of the 40 hours. The trainee must pass both exams.

The third-party security service provider, in conjunction with Equinix, has developed a "scorecard" program for monitoring the performance of the security officers. The scorecard targets key performance indicators (KPIs) that are focus areas mutually agreed-upon between the third-party security service provider and Equinix. In each category, "tools" have been developed to help manage the improvement process. The use of the scorecard and tools are closely monitored and tracked.

Facility and Environmental Protection

Each IBX facility is built to meet required local building codes. When construction of an IBX facility is completed, local government officials perform inspections before a certificate of occupancy is issued. Significant changes to the IBX facility require permits, and IBX facilities are thus re-inspected for building code compliance. Equinix has comprehensive insurance property coverage for IBX facilities by a licensed property insurer covering assets falling in the category of high risk.

The overriding criteria in the build of Equinix IBX facilities are that critical mechanical and electrical components are designed with adequate redundancy. A loss of any critical equipment will not affect customer loads or environmental conditions. During design, the possibility that a critical system is shut down for maintenance and that a failure of another system component occurs at the same time is considered.

IBX facilities meet applicable state, local and federal regulatory requirements for environmental health and safety, including written emergency response plans, emergency contacts notification, inventory of hazardous chemicals, personal protective equipment, chemical spill kits, and hazard communication/warning signage. Emergency standard operating procedures contain documentation about the emergency procedures that address fires, bombs threats, severe weather, and medical emergencies. Other policies and procedures are in place to help ensure that IBX facilities have a consistent level of facility and environmental protection.

Equinix has a safety program composed of IBX "Safety Teams" and a headquarters-based "Safety Core Team." This safety committee functions as an advisory body which periodically audits the existing program, recommending updates or changes as the need arises. To help ensure the safety of persons in the IBX facilities, Equinix relies on customer, contractor, and visitor cooperation with safety guidelines.

Control and Monitoring Systems

A BMS is in place at the IBX facilities in scope. The BMS is a control, monitoring and reporting system used to monitor and control the environmental systems and alert IBX staff to potential issues. Engineers routinely use it to review operating conditions, including temperatures, flows, pressures, electrical and mechanical loads, alarms, etc., looking for abnormal conditions. The BMS also provides long-term data storage to assist in troubleshooting, if needed. The facility environmental systems are monitored and managed by these facility engineers who can be reached on a 24-hour basis via cell phone or another telecommunications device.

This BMS system monitors/controls the following:

- Power systems, including critical electrical components, generators, transfer switches, main switchgears, power distribution units (PDUs), automatic static transfer switches (ASTS), and UPS equipment;
- The HVAC system, which controls and/or monitors space temperature and humidity within the IBX facilities, space pressurization, HVAC equipment status and performance, and outside air conditions;

- Fire detection and suppression equipment, such as very early smoke detection apparatus (VESDA), double interlock pre-action and detection systems, and zoned gaseous-based fire extinguishing system; and
- Leak detection systems.

Experienced technicians perform regular equipment checks and maintenance procedures per defined schedules to help ensure that fire detection and suppression, power management, and HVAC equipment is working properly. In addition, IBX staff performs and logs visual checks of power, environmental, and other system controls, including battery and fuel monitoring systems per defined schedules. Insurance is also in place for such critical equipment.

Fire Detection and Suppression

Equinix IBX facilities are constructed with fire detection and suppression systems that limit potential damage in the event of a fire. Key features of the fire detection and suppression system varies by the IBX location and includes a combination of any of the following:

- Multi-zoned, dry-type, double interlock pre-action fire suppression system
- Laser-based VESDA
- Dual alarms (heat and/or smoke) activation
- Zoned gaseous-based fire extinguishing system

Sprinkler systems in the IBX facilities are implemented with double interlock pre-action and detection systems. The systems are designed such that water does not enter the sprinkler system piping during normal operations. Pre-action detection with intelligent heat detectors are installed in the ceiling of mission critical areas of the IBX facilities. Upon activation of any of these heat detectors, audio-visual alarms (horn and/or strobes) will activate throughout the space. A signal will be sent to a pre-action valve for the affected fire zone. If the temperature in the at-risk area also reaches levels to melt any of the sprinkler head fusible links, water is triggered to enter the sprinkler pipes for the affected areas of the IBX facility.

Fire extinguishers are positioned throughout each IBX facility. Dry chemical or clean agent extinguishers are installed in the mission critical space or adjacent areas where one might reasonably expect a person to carry them into the affected areas during an emergency.

The fire suppression system is monitored on a 24-hour basis by an external alarm monitoring company, which will dispatch the city fire department upon receipt of an alarm. Inside the IBX facilities, software is used for fire detection and monitoring, combined with customized floor plan graphics to illustrate detection devices and fire zones to aid IBX personnel and the fire department in responding to and coordinating fire control activities.

Power Management Utility and Backup Power

Each IBX facility is supplied with high-voltage electrical power from the local utility company. Power enters the facilities from the local utility and is configured at 480 volt, three phases. Where possible, two independent utility sources are in place, originating from independent feeders or substations. Each IBX facility is powered by a dedicated utility step-down transformer for each service. The incoming power is fed into a power system providing diverse power distribution to the cabinet areas.

The incoming service is connected to an ASTS which is also connected to redundant standby diesel generators. Electrical loads are automatically transferred to the standby generators whenever there is a loss of the utility source.

The IBX facilities provide a minimum of N+1 redundancy for every IBX power system to help ensure uptime availability to the customers.

The mission critical electrical loads at each IBX facility are sourced by redundant static or rotary UPS systems, which are configured with automatic static bypass and manually operated full maintenance bypass circuits. The primary UPS systems operate as an online power supply. The UPS systems provide conditioned, uninterruptible power to critical electrical loads. Customer critical loads are protected by an alternate UPS through the use of

ASTS. Web-based reporting services monitor UPS batteries and provide regular battery-automated reporting analysis to the sites that measures the impedance of each jar in a UPS battery system. Impedance trends are used to monitor the health of each jar and to assist in replacement scheduling. The system is also used to monitor ambient temperature of the battery rooms/cabinets in order to verify proper environmental conditions.

UPS systems prevent power spikes, surges, and brown outs while redundant backup diesel generators provide power to the data center in the event that public utility fails. The electrical system has built-in redundancy to help ensure continuous operation. Where UPS batteries are not used, Equinix utilizes continuous power supply using flywheel technology.

Equinix makes use of ASTS in combination with power management modules (PMMs) or PDUs to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring, and control of power to internal and customer computer loads.

Equinix has diesel engine generators in place at each IBX facility to provide emergency power. Generators may be located indoors or outdoors depending on site-specific conditions. Base tanks or "day tanks" provide sufficient fuel storage for ensuring generator startup and run until the main fuel tanks are activated.

Separately installed main fuel tanks provide a source of fuel to engine generators. There is fuel storage on site sufficient for at least 48 hours of design load operation, unless limited by local authorities. Equinix has contracts with multiple fuel providers for the fuel supply.

HVAC

Each IBX facility is designed with HVAC systems to provide stable airflow for the proper control of temperature and humidity. Air handling is provided by means of several different cooling technologies and deployed as a homogenous design at the IBX facilities. The designs can be chilled water closed-loop systems feeding multiple air-handling units or direct expansion refrigerant-based units. To minimize downtime due to equipment failure, major equipment in the HVAC system is designed with a minimum N+1 redundancy. Current design for new sites calls for N+2 redundancy.

A representative HVAC system at an IBX facility would include the following:

- Condenser pumps
- Centrifugal chillers
- Cooling towers
- Primary chilled water pumps or air-cooled condensers
- Air handling units in the collocation area

Each IBX facility is built with zoned temperature control systems. Equinix maintains multiple air handling units at each IBX facility to verify correct temperature and humidity in critical areas. The air handling units in conjunction with a central HVAC plant work to maintain temperature and humidity levels. The average temperature of the supply air to each zone is maintained between 66 degrees and 74 degrees Fahrenheit. If the temperature or humidity varies outside preset limits, an alarm is generated, and facilities personnel are notified. In some cases, to meet customer needs in high-density equipment areas, the supply air temperature to a region may be lower than 66 degrees.

Leak Detection System

A leak detection system is installed, surrounding the "at-risk" areas within the building that monitors for water. Each IBX facility (except IBX SV5, which does not utilize computer room air conditioning units because this IBX facility has a custom-built in-house cooling plant) defines their "at-risk" areas as may be relevant, per the way each IBX facility is designed. The leak detection system is monitored by the BMS.

Maintenance of Critical Systems

The manager facility operations (MFO) or a site engineer makes regularly scheduled rounds. The rounds made are staggered to help ensure maximum equipment coverage.

Prior to the morning rounds, the site engineer prints out a report from the BMS indicating alarm conditions, colocation area temperature and humidity readings, chiller loads, equipment statuses, and electrical loads from the previous night. During rounds, the data on the report is compared to observed conditions. Where necessary, supplemental equipment log sheets are kept manually.

Equinix maintains its facilities via a comprehensive, coordinated program of preventive and predictive maintenance. Maintenance activities are fully scripted, scheduled, reviewed, and approved by operations and engineering management prior to execution of the work.

Equinix's goal is to provide customers approximately 30 calendar days advance notice of planned preventive maintenance activities on critical facility infrastructure systems (such as UPS systems, batteries, and load-transfer equipment, etc.). When expedited maintenance or repair is required, Equinix provides approximately three to seven days advance notice to customers. When urgent repair is necessary, the advance notice to customers could be from zero to three days, with three days as the target.

Whenever possible, preventive and predictive maintenance activities are planned and performed in a manner that is transparent to customer operations. The redundancy features and design of the Equinix IBX critical infrastructure systems allow performance of preventive maintenance without interruption of critical customer loads.

The IBX operations engineering staff performs routine preventive and predictive maintenance. The Equinix computerized maintenance management system, Maximo, is used to schedule the work, issue work tickets, track costs, and record maintenance history. Routine preventive maintenance includes work, such as lubrication, filter changes, and operational inspections, etc. Predictive maintenance (PdM) includes infrared scans, water treatment systems analysis, eddy current testing, and vibration analysis, etc. Outside contractors will be used for some PdM tasks, as determined by the MFO.

Logical Access, Authentication and Authorization

Documented global logical access security policies are in place to specify standard requirements across the organization for how logical access to Equinix's information systems is to be maintained and managed. To access the network, users must first authenticate through a VPN gateway and establish an encrypted connection. VPN gateway devices are configured to enforce two-factor authentication based upon the user's unique network domain credentials and a digital certificate assigned by Equinix and installed locally on the user's device. All network users, remote or on-premise, are required to authenticate to the VPN gateway prior being granted access to Equinix's network domain. Global group policies (GPOs) are utilized to govern predefined user account and minimum password requirements for all network domain user accounts. Authentication to application and web server operating systems is granted based on the user account's domain credentials. Authentication controls are inherited from the primary domain controller's GPOs. Application and database users are authenticated via user account and password. Administrative privileges to the network domain, operating systems, databases, and applications are restricted to authorized personnel.

Logical Access Requests and Access Revocation

Corporate IT personnel are responsible for administering and provisioning user access privileges to the network and underlying operating system and databases supporting the in-scope systems. As a component of the onboarding process, regional human resources (HR) department personnel create a profile for new hires employees within the corporate human resources management (HRM) system, which triggers an alert notification to be sent to corporate IT personnel to create a new network user account for the employee. User account privileges are assigned based upon least privilege. Changes to user access including the assignment of elevated access permissions, requires manager approval. IT personnel revoke system user access privileges for exit employees upon receipt of the notification triggered by HR personnel terminating the user within the HRM system. The process of revoking a terminated user's system access is documented within a help desk ticket.

Change Management

A change control process is documented and in place to address planned and emergency changes to the in-scope systems. A formal change request must be submitted which could include details such as change category, region affected, functional area, and classification. Change requests are reviewed and discussed during the weekly change review meeting prior to development. Once approved, a ticket is opened, and the

change is assigned to a technical resource for development. After development, the changes are tested in a quality assurance (QA) environment that is segregated from development and production. Unit, functional, integration, and user acceptance testing may be performed based on the type of change. After the relevant testing is completed and approved, the change is pushed to production and released in the subsequent application release window.

Data Backup and Disaster Recovery

IT disaster recovery has been designed to address the recovery of Equinix's technology assets. Backup / failover capabilities of Equinix's internal processes exist between its own data centers. Critical systems rely on backup data as part of the disaster recovery plan. Backup frequency varies, and application data determined to be of medium to very high data criticality are backed up at least daily. The type of backup differs based on application, database, program, system, and network data. Backup data is stored at the disaster recovery site.

Equinix conducts a variety of tests to ensure continuity of critical business processes. Testing at Equinix IBX data centers includes, but is not limited to, scheduled preventative maintenance tests on critical infrastructure to ensure proper fail-over to backup systems; dynamic monitoring of critical infrastructure for proper performance; scenario-based tests for staff; and evacuation drills. All tests are followed up with a post-test analysis and extensive reviews, which are communicated to management.

Incident Response

Incident response and escalation policies and procedures are in place to manage unexpected incidents impacting the business. The procedures are reviewed on a periodic basis to ensure they are still effective in meeting the business objectives. The procedures outline the following:

- Assignment of roles and responsibilities for execution of the incident response program
- Incident identification, investigation, and triage
- Communication protocols and timing to affected parties
- Remediation (containment, eradication, and recovery)
- Post incident activities (restoration and lessons learned)

Management utilizes an enterprise ticketing system for documenting, communicating, and collaborating to resolve any identified incidents with customers. Information security personnel complete a root cause analysis upon system outages that include the incident and impact analysis, resolutions, lessons learned, and action items. Data center facility incidents and corrective measures are reported on monthly for management review to ensure that the incident response procedures were followed and that the incident was resolved. Corrective measures or changes that occur as a result of incidents and identified deficiencies follow the standard change control process.

Incident response plan testing exercises using simulated security incidents are performed at data center facilities at least annually and the results are documented to assess the effectiveness of the process. An incident management training program in place to promote incident response plan awareness. Data center operations personnel are required to participate in the training program at least biennially to help ensure that they understand their roles and responsibilities for incident response.

A crisis management plan has also been implemented for the response to cyber security incidents that could result in potential data breaches impacting cross-functional operations and system globally. A global crisis management team (CMT) meets on an annual basis to review the plan and perform tabletop exercises to assess the team's ability to effectively response to cyber incidents. CMT personnel are also educated on the latest cyber threats and vulnerabilities that could potentially impact the company during the annual meeting.

IT Systems Monitoring

Equinix's IT security team has implemented a centralized security information and event management (SIEM) application to monitor and log certain security event for the in scope systems. An intrusion detection system (IDS) is also in place to monitor and analyze network traffic. The SIEM and IDS are configured to alert IT personnel in the event of predefined policy conditions being met including possible or actual security breach events.

A next generation antivirus / antimalware system is also in place to provide detect and prevent the transmission of malicious files or programs within the network. The next generation endpoint protection software is installed on a centralized server and is configured for automatic updates and real-time scans for registered Windows servers and workstations.

Disaster Recovery

A Business Recovery Plan (BRP) represents actions to be taken by the IBX operations and physical security business areas at Equinix IBX facilities that focuses on an impact to the facility, applications/systems, employees, and external parties. The plan addresses a local incident but does not address a regional disaster, with multiple IBX's impacted simultaneously. The BRP addresses the following plan objectives:

- Minimize business losses resulting from disruption to business processes.
- Provide a plan of action to facilitate an orderly recovery of critical business processes.
- Identify key individuals or teams who will manage the process of recovering and restoring the business after an incident or disaster.
- Specify the critical business activities that need to continue after an incident.
- Outline the logistics of recovering critical business processes.

The Business Continuity Program Office is responsible for overseeing the Business Continuity Management Program. Quarterly and annual reminders are sent to Global Operations Support, who in turn require each site to update their plan. Copies of the plan are maintained at each IBX facility in hard copy binder, and on the regional Operations SharePoint site and made accessible to the Business Continuity Plan Program Office. Global Operations Support schedule and conduct exercises on the BRP.

Plan Responsibility and Maintenance		
Responsibility	**Frequency**	**Owner**
Maintain Emergency Contact List for current employee and vendor contact information.	Quarterly	IBX Manager
Review Threat & Risk Assessment and Business Recovery Plan and advise Global Ops Support of required updates.	Annually	IBX Manager
Review workaround procedures and advise Global Ops Support of required updates.	Annually	IBX Manager
Conduct "war games", record results, and distribute to country management team.	Annually	IBX Manager – for connectivity Facilities Manager – for mechanical, electrical, and plumbing (MEP) infrastructure
Conduct "Black Start" test, record results, take corrective action.	Monthly	Facilities Manager – for MEP infrastructure
Conduct "What If" scenarios exercises, record results, take corrective actions.	Monthly	IBX Manager – for connectivity Facilities Manager – for MEP
Conduct "Pull the Plug" test, record results, take corrective action.	Annually	Facilities Manager – for MEP infrastructure
Plan and conduct IBX application and system exercises (Local Servers).	Annually	IT and IBX Manager

Plan Responsibility and Maintenance		
Responsibility	**Frequency**	**Owner**
Plan and conduct IT application and system exercises (Enterprise servers).	Annually	Global IT
Plan data retention	7 years from last update	Global Ops Support

Data

Customers are responsible for the data maintained within their environments. Within the scope of the Data Center Hosting Services system, customers can manage and monitor their services, submit new requests, and view the status of open requests by logging into the ECP. In addition, the portal is used to allow customers the ability to manage their accounts and to view when any service delivery impacting maintenance begins and when it is completed.

Internal data sources captured and utilized by Equinix to deliver its data center hosting services, includes, but it not limited to, the following:

- Biometrics, proximity card, and PIN code access history logs, including access history and security alarms.
- CCTV recorded footage is maintained for 90 days, and at minimum 30 days.
- Alert notifications and monitoring reports generated from the environmental monitoring applications and the BMS.
- Incident/issue reports documented via the ticketing systems.

Significant Changes During the Review Period

On October 11, 2019, Equinix completed the sale of its former New York 12 (NY12) data center facility located in Piscataway, New Jersey, to Verizon. The transaction included the customer deployments associated with the site. NY12 tenants were notified and will continue to operate at the site under Verizon's ownership. No other significant changes to the Data Center Hosting Services system occurred during the review period.

Subservice Organizations

Equinix utilizes Digital Realty Trust for environmental protection controls at the Chicago 4 (CH4) data center facility the physical security controls at the Dallas 10 (DA10) data center facility. The services provided by Digital Realty Trust were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Digital Realty Trust, alone or in combination with controls at Equinix, and the types of controls expected to be implemented at Digital Realty Trust to achieve Equinix's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Digital Realty Trust	Applicable Trust Services Criteria
Digital Realty Trust is responsible for ensuring that physical access to the Dallas 10 (DA10) data center facility (including colocation space, backup media storage and other sensitive locations as well as sensitive system component within this locations) is restricted authorized personnel.	CC6.4 – CC6.5

Control Activity Expected to be Implemented by Digital Realty Trust	Applicable Trust Services Criteria
Digital Realty Trust is responsible for the environmental protection controls design, development, implementation, operations, maintenance, and monitoring to meet availability commitments and requirements at the Chicago 4 (CH4) data center facility.	A1.2

CONTROL ENVIRONMENT

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

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 Equinix's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Equinix's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. 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 Equinix's values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Equinix has implemented in this area are described below.

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel are documented within the employee manual.
- Employees are required to sign an acknowledgment form indicating that they were given access to company policies and procedures and the employee manual, and understand their responsibility for adhering to the requirements outlined within the policies, procedures, and manual.
- New hires are required to sign an employment contract agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks are performed for North America employee candidates as a component of the hiring process.

Senior Leadership Oversight

Equinix recognizes that effective information security management is critical to its business and customers, and strives to continually deliver high-level service that includes protection of both Equinix and customer assets from internal and external threats. The Equinix board of directors and senior management team are dedicated to creating and executing appropriate security policies company-wide. To ensure its information security management program is fully integrated and supports all business requirements, Equinix's chief information security officer has been appointed by the board of directors and senior leadership to define and implement specific security-related policies, which are annually reviewed and endorsed by the senior management team. Equinix's senior management team also commits to the following oversight activities:

- Setting policy objectives focused on reducing risk and identifying acceptable information security risk levels, and establishing overarching company policy relating to information management, hardware, firmware, and software.

- Implementation of a systematic approach to risk assessment and methods for minimizing the risks of damage to company assets, information, reputation, hardware, software, and data; and suited to compliance and regulatory requirements.
- Promoting staff-wide compliance with security policy requirements, and ensuring Equinix employees and computer systems do not infringe on any copyright or licensing laws.

All Equinix managers, employees, and contractors are trained and responsible for complying with company policies. Corporate and operating unit management are responsible for establishing and maintaining internal controls and promoting integrity and ethical values to company personnel. Dedicated regional security and compliance teams are in place help to assess the controls and operations within business units and report the results of control assessments to executive management teams. In addition, security and compliance teams help to advise operations management on risk assessment and mitigation activities, including the identification and implementation of controls. These activities are orchestrated and facilitated through the company's information security management system (ISMS) established for the management of the risks to the organization's information security objectives. The information security management committee (ISMC), comprised of members of top management, meets at minimum, on an annual basis, to review security, compliance and operational metrics related to the achievement of its information security objectives, and their continued alignment with the company's mission.

Organizational Structure and Assignment of Authority and Responsibility

Equinix's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Equinix's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Equinix 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.

Equinix's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

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. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts and position descriptions are communicated to employees and updated as needed.

Commitment to Competence

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

- Documented human resources policies are maintained to guide human resources personnel during hiring and termination processes. Procedures are in place to help sure are in place to help ensure that specific elements of the hiring and terminations processes are consistently executed.
- Pre-hire screening procedures are utilized to include the following:
    - Review of candidate's resume;
    - Interview(s);
    - Skills testing, as applicable;
    - Reference checks; and

    - Background screening including education and employment verification (North America).
- A third-party web application is utilized during the hiring process to qualify the skills of applicants within certain job functions.
- Position requirements are translated into written required skills and knowledge levels based on competence levels for particular jobs.
- Personnel are provided with orientation, hands-on training and supervision to the extent deemed necessary by management. Personnel are also required to complete new hire security awareness training and annual security awareness training thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Performance evaluations are conducted for employees at minimum, on an annual basis, conducted to help ensure employees are meeting their goals and objectives as outlined during the annual review process; human resources personnel utilize a third-party application to track the completion and receipt of employee evaluations.

Accountability

Equinix has defined accountability as holding individual's onus for their internal control responsibilities. Accountability encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and establishing policies and practices that relate to employee training, evaluation, counseling, promotion, compensation, and remedial actions. Specific control activities that Equinix has in place for this area are described below:

- Management conducts a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.
- Employee sanction policies are documented to communicate consequences for disciplinary actions, up to and including termination, for violations to company policies and the code of conduct.
- A whistleblower protection policy and ethics and compliance hotline are in place for employees to anonymously report violations, complaints or concerns related to company policies and the code of conduct.

Risk Assessment

Equinix's the process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. The ISMC oversees risk management ownership and accountability. Operations management from different operational areas are involved in risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

A standard risk assessment template (IBX threat and risk assessment survey) is utilized globally to ensure that key inputs are factored in consistently across Equinix's data center locations. A risk assessment is performed for each data center site and field office on an annual basis for formal review and approval by the ISMC, and any risk owners who have been assigned a risk treatment plan. In addition to the scheduled annual assessments, Equinix has identified the following as reasons for prompting an ad hoc risk assessment to be performed:

- Significant changes to the business affecting information security;
- A new contract involving modified information security requirements; and
- After an information security incident.

Objective Setting

Equinix considers the needs and expectations of interested parties and the boundaries of its data center hosting services system, which includes the identification and analysis of risks that pose a threat to the organization's ability to provide reliable services to its customers. The first step of the process is determining the organization's objectives is an essential part of the process and understanding the potential threats and vulnerabilities that could the threaten its ability to achieve said objectives. Senior leadership and operation management has committed to customers to carry out certain objectives in relation to the data center hosting services provided. These commitments are documented and formally reviewed by the ISMC to help ensure that its business objectives related to operations, reporting, compliance, are aligned with the company's mission, and are utilized for the annual risk assessment process.

Risk Identification, Analysis, and Mitigation

The risk assessment process includes a systematic approach of estimating the magnitude of risks and the process of comparing the estimated risks against risk acceptance criteria. The approach is comprised to three overarching components: risk identification, risks analysis/evaluation, and risk mitigation; to ensure repeatable risk assessment procedures that produce consistent, valid, and comparable results.

Risk Acceptance Criteria

Risk acceptance criteria have been established consisting of a point-based risk scale, being split into three priority levels; High, Medium, and Low. The criteria for information security risk acceptance are detailed as follows:

Residual Risk	Risk Priority	Notes	Risk Treatment Options
>5.0	High	Approval required from risk owner Unacceptable Will be prioritized for treatment	Avoid, Mitigate, and/or Transfer
2.0 – 5.0	Medium	Approval required from risk owner Will not be prioritized for treatment but will be assessed for risk reduction in pursuit of continual improvement	Accept, Avoid, Mitigate, and/or Transfer
Below 2.0	Low	Approval required from risk owner Acceptable Will not be prioritized for treatment but will be assessed for risk reduction in pursuit of continual improvement	Accept

Acceptable risk treatment options are documented for each risk priority level. Risk treatment options include:

- *Accept* - No corrective action; document acceptance decision and monitor.
- *Avoid* - Cease activity to eliminate risk.
- *Mitigate* - Corrective action to eliminate or reduce impact or likelihood.
- *Transfer* - Shift impact to other parties, e.g. insurers, suppliers.

Equinix defines information security assets as anything tangible and intangible at its data center facilities that has value and requires protection. The risk assessment procedure, and threat and risk assessment surveys for each data center facility on an annual basis identifies five major hazard categories along with examples for each category. The five hazard categories outlined by Equinix include natural, man-made, site infrastructure, health, and economical / political threats. The operations manager completing the survey may include additional risks within each hazard type specific to their site, as needed.

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

External Factors

- Technological developments that could affect the nature and timing of research and development
- Changing customer needs or expectations that could affect services provided and customer service
- 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 and highlight the need for contingency planning
- Economic changes that could have an impact on management decisions related to financing, capital expenditures and expansion

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing that could adversely affect the entity's operations
- The quality of personnel hired, and methods of training utilized and motivation that could influence the level of control consciousness within the entity
- Changes in management responsibilities
- The nature of the entity's activities, and employee accessibility to assets, that could contribute to misappropriation of resources

Risk definitions are included with the threat and risk assessment survey worksheets, including instructions to enable the persons completing the survey worksheet to apply a value for calculating risks, as well as mitigation measures, in a uniform manner, based on:

- Probability
- Risks
    - Human Impact (HI)
    - Properly Impact (PI)
    - Business Impact (BI)
- Mitigation measures
    - Planning and preparedness
    - Internal Resources
    - External Resources

The threat and risk assessment surveys worksheet completed for each site are required to include descriptions of mitigation measures as well as identify the risk owners responsible for agreeing risk treatment and residual risk. The surveys completed for each site are also required to identify the protections in place for functional area level information security assets.

Formulas embedded in the threat and risk assessment survey worksheets are utilized to calculate an inherent risk total to assess the likelihood of untreated risks, based on probability, human impact, property impact, and business impact factors for each hazard:

Value	Probability (P)	Human Impact (HI)	Property Impact (PI)	Business Impact (BI)
0	Not applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0
1	Improbable occurrence – could not conceivably happened or expect to happen less than once in 100 years.	Negligible – no first aid required	Negligible – negligible damage	Negligible – no direct damage to business delivery (US$0-$135 / €0-100)
2	Possible occurrence – expected to happen once or more every 10 years *(Note: Includes 1 – 10 years).*	Insignificant – slight injury requiring on-site first aid	Insignificant – insignificant damage; structural integrity not affected	Insignificant – minor damage to business delivery; customers not harmed (US$135-$1350 / €100-1000)
3	Occasional occurrence – could happen, but rarely. Expected to occur annually or every 6 months.	Slight – one person requiring hospital treatment	Slight – slight damage; structural integrity not affected	Slight – minor damage with single customer affected (US$1350-$13,500 / €1000-10,000)
4	Frequent – could happen monthly / quarterly.	Significant – multiple injuries requiring hospital treatment	Significant – some property damage or loss, including moderate structural damage	Significant – parts of business delivery damaged; multiple customers involved (US$13,500-$135,000 / €10,000-100,000)
5	Regular occurrence – could happen weekly / monthly.	Considerable – death and/or serious injury	Considerable – extensive property damage or loss; structure requires extensive repairs	Considerable – business delivery seriously damaged, >80% customer involved (US$135,000-$1350,000 / €100,000-1,000,000)
6	Common occurrence – could happen daily / weekly.	Catastrophic – multiple deaths and/or serious injuries	Catastrophic – almost total damage or loss; facility must be torn down and replaced	Catastrophic – no business delivery possible (>US$1,350,000 / €1,000,000)

The mitigation measures in place for planning and preparedness, internal resources, and external resources, are also considered and mitigation values are utilized to reduce the overall score when calculating the residual risk totals. The criteria established for risk acceptance is a Residual Risk Total of 2.0 or lower.

Value	Planning and Preparedness (PP)	Internal Resources (IR)	External Resources (ER)
0	Not Applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0
1	Non-existent – No planning or procedures developed to deal with the incident	Non-existent – No internal capability to deal with the incident	Non-existent – No thought given to utilizing outside suppliers / vendors / third parties

Value	Planning and Preparedness (PP)	Internal Resources (IR)	External Resources (ER)
2	Very weak – some planning initiatives under way but not implemented at this time	Very weak – significant gaps in resources for responding to the incident	Very weak – no outside suppliers / vendors / third parties capable of responding to the incident
3	Weak – some planning initiatives under way but gaps identified	Weak – some resources available but gaps identified	Weak – suppliers /vendors / third parties have significant gaps in capabilities, equipment, and / or location of external suppliers / vendors / third parties
4	Adequate – partial equipment in place; procedures are in development	Adequate – personnel trained, with minor gaps in some areas	Adequate – suppliers / vendors / third parties competent to respond to a single incident but may be overwhelmed by incidents affecting multiple sites
5	Strong – good equipment; procedures exist, with minor gaps in some areas	Strong – personnel trained but not yet equipped	Strong – competent suppliers / vendors / third parties available, with some limitations to equipment or pre-event planning
6	Very strong – emergency/alternate equipment in place and fully operational; procedures fully developed; regularly tested	Very strong – trained and equipped personnel available	Very strong – competent alternate suppliers / vendor / third parties available with capability to respond to major events, and pre-event planning in place

The level of risk determined for each hazard is indicated in each region and/or country's IBX's threat and risk assessment survey register. The results of risk calculation are compared with the risk criteria established to prioritize the calculated risks for risk treatment.

During the risk evaluation process, the appropriate risk treatment option is selected and all controls that are necessary to implement the information security risk treatment option are chosen. Each risk treatment plan is assigned a risk owner, and the risk owner provides their approval of the risk treatment plan by formally reviewing the risk assessment which details the risk treatment plan(s). Evidence of these approvals is retained in the risk assessment spreadsheet. The key control matrix is updated and the risk treatment plan is documented. The risk owners' approval for the risk treatment plan is received. Once the risk treatment has been completed, the risk owners accept any residual risk.

Potential for Fraud

Management realize that that the potential for fraud can occur when employees are motivated by certain pressures or temptations 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 risk assessment process considers the potential for fraud hazards, and documented the documented risk assessment policies and procedures include guide personnel in identifying and analyzing risks including the potential for fraud. A risk assessment is performed on an annual basis that considers the potential for fraud.

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 results of the risk assessments are utilized by the ISMC to prioritize the information security risks and take the appropriate actions for implementing controls selected mitigate against risks to an acceptable level. Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk.

The applicable trust 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 criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Equinix's description of the system.

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

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the Data Center Hosting Services system.

INFORMATION AND COMMUNICATION SYSTEMS

Equinix's internal systems supporting the data center hosting services include Dell Blade servers running on Windows and Red Hat Enterprise Linux operating systems. These internal systems are used to:

- Maintain customer information, work requests, and work history for the data center sites
- Design and dispatch orders to site operations and maintain information regarding utilized site assets
- Monitor customer service infrastructure
- Schedule and track maintenance on site infrastructure
- Collect, dispatch, and track customer support requests
- Identify on-call engineering resources for incident response and support escalation
- Track and identify customer port assignments

- Manage customer order workflow within operations
- Design site infrastructure layout for customer solutions
- Manage site security access control
- Record and monitor CCTV in each site

Equinix utilizes both formal and informal methods for corporate-wide communication. Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within the organization. Management holds meetings bi-weekly via phone and quarterly in person to share information at a business level. Departmental staff meetings are held on a periodic basis to discuss operational issues.

Internal Communications

Equinix has implemented various methods of communication to help provide assurance that all employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for all employees, and the company intranet to communicate time-sensitive information. Employees are encouraged to communicate to their supervising manager or, if needed, directly with executive management.

External Communications

Equinix has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include periodic e-mail messages, application version release notes, and through direct relationships with Equinix personnel. If incidents are communicated through the online portal, personnel follow documented incident response plan. All incidents are processed according to Equinix global procedures following the Equinix global incident flowchart. All incidents are documented within the ticketing system and tracked by management until resolved.

MONITORING

Management monitors controls to consider whether they are operating as intended and that the controls are modified for changes in conditions. Equinix's management performs monitoring activities to continuously assess the quality of internal control over time. Equinix management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control activities and procedures. Equinix's management places emphasis on maintaining sound internal controls, as well as, ensuring integrity and ethical values to Equinix personnel.

Ongoing Monitoring

Equinix utilizes third-party assessors to query the customer base across a variety of topics intended to gauge business performance. Internal customer assessments are made at random and are specific to an order, trouble ticket, escalation request, etc. to which the customer was recently serviced. By examining and trending the results, Equinix continually strives to improve the customer experience.

Equinix has implemented a site operations quality control program. This program is a vital element of the day-to-day operations of the Equinix facilities. The program provides a means for senior management to effectively determine the compliance of established Equinix standards at the site level. Additionally, a comprehensive root cause analysis system is utilized to provide senior management in the identification of underlying causes of identified deficiencies and assist in developing proactive resolutions.

Equinix monitors third-party providers and subservice organizations as part of the daily IT business operations.

Separate Evaluations

Equinix understands the importance of established procedures and processes in performing the daily duties demanded by the business. Repeatability is essential to the customer experience being consistent and setting the expectation against established service level agreements. The customer knows fully what to expect and how long to completion no matter the facility or location of the service being requested. Equinix develops, tests, and constantly reviews established processes and procedures. Management conducts monthly reviews of the documentation to validate accuracy and identify areas for streamlining. Each process or procedure is assigned an owner to document accuracy and applicability to the product, service, and business as a whole. Revisions are made to the documents and released using an operations bulletin process. The operations bulletins denote behavioral or process changes and the gains from those changes. Each operations bulletin is logged and filed in the site library.

Internal and External Auditing

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

- SOC 1 / ISAE 3402 and SOC 2 Examinations
- ISO 27001 and ISO 90001 (RJ1. RJ2. SP1, SP2, SP3, SP4 and BG1)
- ISO 22301
- SAP Cloud Infrastructure Operations
- Tier III Design, Facility and Operations
- Environmental Health and Safety Standards
- National Institute of Standards and Technology (NIST) 800-53
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley (SOX)

Subservice Organization Monitoring

Equinix's CH4 data center facility is located in the same multi-tenant building as the CH1 and CH2 data center facilities. Facility engineers and security personnel located on-premise at the adjacent CH1 and CH2 data centers are tasked with directly monitoring the CH4 facility and the environmental protection system controls provided by Digital Realty Trust. Equinix personnel perform daily walkthrough visits of facility and monitor facility activity through the use of 24x7 security monitoring and digital surveillance cameras. Equinix operations personnel local to the Dallas metropolitan area are tasked with directly monitoring the DA10 facility and the physical access control services provided by Digital Realty Trust. Monitoring activities performed by Equinix include periodic user access reviews of the DA10 physical access control system, as well as regular facility walkthrough visits by local IBX managers and facilities engineers. Services provided by Digital Realty Trust are also monitored through phone and e-mail communications, meetings, and the service provider's customer web portals.

Evaluating and Communicating Deficiencies

The nature, timing and extent of deviations or deficiencies identified by the site personnel are logged and input into a site issues database. The database serves to assign ownership of the issue, track progress and report completions as needed to maintain the highest level of performance at the site level.

Corrective actions or changes to established documents or procedures are announced to affected areas by two means of communications. An operations information brief is used to alert operations personnel of new information and announce new initiatives from the company or the operations management team. Should the

announcement be significant as to alter existing documentation, processes, procedures, or behavioral aspects of Equinix's daily duties, the operations bulletin is the vehicle for announcement.

Operations bulletins are mandatory for compliance and are often time sensitive. Each operations bulletin contains an effective date and advises of special instruction needed for successful performance.

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the 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 Hosting Services system provided by Equinix. The scope of the testing was restricted to the Data Center Hosting Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period, November 1, 2018, through October 31, 2019.

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 review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

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

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

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

Sampling

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

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

Reliability of Information Provided by the Service Organization

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

Test Results

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

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Equinix's code of conduct is included within the employee manual to communicate company values and behavioral standards to personnel.	Inspected the employee manual to determine that Equinix's code of conduct was included within the employee manual to communicate the company's values and behavioral standards to personnel.	No exceptions noted.
CC1.1.2	Employees complete an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.	Inspected the signed policy acknowledgments for a sample of employees hired during the review period to determine that each employee sampled completed an acknowledgement form indicating they had been given access the employee manual and understood their responsibility for adhering to the code of conduct outlined within.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	New hires are required to sign an employee agreement consenting to not disclose confidential or proprietary client and company information to unauthorized parties.	Inspected the signed employee agreements for a sample of employees hired during the review period to determine that each employee sampled singed an employee agreement consenting to not disclose confidential or proprietary, client and company information to unauthorized parties.	No exceptions noted.
CC1.1.4	Background checks are performed for employees as a component of the hiring process.	Inspected the background check documentation for a sample of employees hired during the review period to determine that a background check was performed 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	The board of directors and senior management team has assigned authorities for defining and implementing security policies, to the chief information security officer.	Inspected the Equinix Security Policy statement to determine that the board of directors and senior management team had formally assigned authorities for defining and implement security policies, related to the achievement of its objectives, to the chief information security officer.	No exceptions noted.
CC1.2.2	An ISMC comprised of members of top management, meets at minimum, on an annual basis to review security, compliance and operational metrics related to the achievement of the organization's information security objectives, and their continued alignment with the company's mission.	Inspected the ISMS organization structure, management review procedure, and the most recent annual management meeting minutes to determine that an ISMC, comprised of members of top management, was in place and met during the review period to review security, compliance and operational metrics related to the achievement of the company's information security objectives.	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	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel. These charts are communicated to employees and updated as needed.	Inspected the company organizational charts and an example update notification during the review period to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel, and that the charts along with updates to the charts were communicated to employees.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills and knowledge levels required for the competence levels of particular jobs.	No exceptions noted.
CC1.3.3	The board of directors and senior management team has assigned authorities for defining and implementing security policies, to the chief information security officer.	Inspected the Equinix Security Policy statement to determine that the board of directors and senior management team had formally assigned authorities for defining and implement security policies, related to the achievement of its objectives, to the chief information security officer.	No exceptions noted.
CC1.3.4	An ISMC comprised of members of top management, meets at minimum, on an annual basis to review security, compliance and operational metrics related to the achievement of the organization's information security objectives, and their continued alignment with the company's mission.	Inspected the ISMS organization structure, management review procedure, and the most recent annual management meeting minutes to determine that an ISMC, comprised of members of top management, was in place and met during the review period to review security, compliance and operational metrics related to the achievement of the company's information security objectives.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	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 new employee hiring workflow procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties.	No exceptions noted.
CC1.4.2	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inquired of the security and compliance specialist regarding the employee training procedures to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
		Inspected the corporate training portal and example training course documentation made available on to employees to determine that training courses were available for specific job functions and roles to maintain and advance the skill level of personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	Employees are required to complete new hire security awareness training and annual security awareness training thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training materials and completion records for a sample of employees hired during the review period to determine that new hire security awareness training was completed for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
		Inspected the security awareness training materials and completion records for a sample of existing employee to determine that security awareness training was completed during the review period for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
CC1.4.4	Background checks that include employment and education verifications are performed for employees as a component of the hiring process.	Inspected the background check documentation for a sample of employees hired during the review period to determine that a background check employment and education verifications were performed for each employee sampled.	No exceptions noted.
CC1.4.5	Management conducts a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.	Inquired of the human resources specialist regarding the employee performance evaluation procedures to determine management conducted a performance review of employee on an annual basis to evaluate individual performance against expected levels of performance and conduct.	No exceptions noted.
		Inspected the most recent annual performance review documentation for a sample of existing employees to determine that an evaluation of individual performance against expected levels of performance and conducts was performed during the review period for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Employee sanction policies are documented to communicate consequences for disciplinary actions, up to and including termination, for violations to company policies and the code of conduct.	Inspected the employee sanction policies to determine that documented employee sanction policies were in place to communicate consequences for disciplinary action, up to an including termination, for violation to company policies and the code of conduct.	No exceptions noted.
CC1.5.2	A whistleblower protection policy and ethics and compliance hotline is in place for employees to anonymously report violations, complaints or concerns related to company policies and the code of conduct.	Inspected the whistleblower protection policy and EthicsPoint portal to determine that a whistleblower protection policy and ethics and compliance hotline was in place for employees to anonymously report violations, complaints or concerns related to company policies and the code of conduct.	No exceptions noted.
CC1.5.3	Management conducts a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.	Inspected the most recent annual performance review documentation for a sample of existing employees to determine that an evaluation of individual performance against expected levels of performance and conducts was performed during the review period for each employee sampled.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Security policies and procedures are documented that identify the information required to support the functioning of internal control and the achievement of objectives.	Inspected the security policies and procedures to determine that documented policies and procedures were in place that identified information required to support the functioning of internal control and the achievement of objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Internal data sources are used to obtain meaningful information to support the functioning of internal control, including the following: • Security monitoring applications, systems and manual reviews • Annual internal audits • Infrastructure and BMS monitoring applications to monitor system availability and capacity levels	Inspected example internal data source reports, logs, and alerts generated during the review period to determine that internal data sources were used for the purposes of obtaining meaningful information to support the functioning of internal control, that included the following: • Security monitoring applications, systems and manual reviews • Annual internal audits • Infrastructure and BMS monitoring applications to monitor system availability and capacity levels	No exceptions noted.
CC2.1.3	External data sources are used to obtain meaningful information to support the functioning of internal control, including the following: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal • Preventative maintenance reports to testing and confirmation the operations of environmental systems • Security KPIs for facilities that employ onsite security guards	Inspected example external data source reports generated during the review period to determine that external data sources were used for the purposes of obtaining meaningful information to support the functioning of internal control, that included the following: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal • Preventative maintenance reports to testing and confirmation the operations of environmental systems • Security KPIs for facilities that employ security guards	No exceptions noted.
CC2.1.4	The entity's global information security group monitors the security impact of emerging technologies and threats, and notifies relevant personnel.	Inspected example IT security subscription service e-mail notifications received during the review period to determine that the entity's IT security and compliance groups monitored the security impact of emerging technologies and that the impacts of applicable laws or regulations were considered by senior management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Documented policies are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies are communicated to internal personnel via the company Intranet.	Inspected the security policy documentation maintained on the internal intranet to determine that documented policies were in place to guide personnel in the entity's security and availability commitments and the associated system requirements, and that the policies were communicated to internal personnel via the company Intranet.	No exceptions noted.
CC2.2.2	Employees are required to complete new hire security awareness training and annual security awareness training thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training materials and completion records for a sample of employees hired during the review period to determine that new hire security awareness training was completed for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
		Inspected the security awareness training materials and completion records for a sample of existing employee to determine that security awareness training was completed during the review period for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
CC2.2.3	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills and knowledge levels required for the competence levels of particular jobs.	No exceptions noted.
CC2.2.4	Documented policies and procedures for reporting incidents are in place to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident management policies, procedures, and workflows to determine that that documented policies and procedures for reporting incidents were in place to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	A change review meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the change review meeting documentation for a sample of weeks during the review period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affected the system for each week sampled.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Equinix's security and availability commitments and the associated system requirements are documented in customer agreements and via IBX product policies published to the company website.	Inspected the signed contracts and nondisclosure agreements for a sample of new customers onboarded during the review period to determine that a signed contract and nondisclosure agreement that included security and availability commitments and system requirements was in place for each customer sampled.	No exceptions noted.
		Inspected the IBX data center policies, product policies, and service level agreements maintained on the company website to determine that Equinix's security and availability commitments and the associated system requirements were documented and communicated via IBX policies published to the company website.	No exceptions noted.
CC2.3.2	Documented policies and procedures are in place to guide personnel in communication with external parties regarding matters affecting the functioning of internal control.	Inspected the incident response policy to determine that documented policies and procedures were in place to guide personnel in communication with external parties regarding matters affecting the functioning of internal control.	No exceptions noted.
CC2.3.3	Changes, incidents, and outages related to security and availability at the data centers are communicated to customer and external users of the system via e-mail advisory notifications.	Inspected example external advisory notifications sent during the review period to determine that changes, incidents, and outages that changes, incidents and/or outages related to security and availability at the data centers were communicated to customer and external users of the system via e-mail advisory notifications.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.4	Customer end-users are provided with access to the ECP and procedures for contacting the GSD to report incidents, concerns, or complaints related security and availability.	Inspected the IBX policies and procedures and GSD contact information published the company website, and the reporting mechanisms made available via the ECP to determine that customer end-users were provided with access to ECP and procedures for contacting procedures for contacting the GSD to report incidents, concerns, or complaints related security and availability.	No exceptions noted.
CC3.0: Risk Management and Design and Implementation of Controls			
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	Documented information security risk management policies and procedures are in place to guide personnel in the identification of relevant operations, security, and compliance objectives of the company.	Inspected the risk assessment policies, procedures, and templates to determine that documented information security risk management policies and procedures were in place to guide personnel in the identification of relevant operations, security, and compliance objectives of the company.	No exceptions noted.
CC3.1.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks related to company objectives. Risks that are identified are rated using a risk evaluation process and formally documented, along with mitigation strategies, for management review.	Inspected the most recent annual IBX threat and risk assessments for a sample of data center facilities to determine that a risk assessment was performed during the review period that considered the identification and assessment of risks relating to the company's objectives, and that risks were identified using a risk evaluation process and formally documented, along with activities, for management review.	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	Documented information security risk management policies and procedures are in place to guide personnel in the identification of relevant operations, security, and compliance objectives of the company.	Inspected the risk assessment policies and procedures to determine that documented information security risk management policies and procedures were in place to guide personnel in the identification of relevant operations, security, and compliance objectives of the company.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks related to company objectives. Risks that are identified are rated using a risk evaluation process and formally documented, along with mitigation strategies, for management review.	Inspected the most recent annual IBX threat and risk assessments for a sample of data center facilities to determine that a risk assessment was performed during the review period that considered the identification and assessment of risks relating to the company's objectives, and that risks were identified using a risk evaluation process and formally documented, along with activities, for management review.	No exceptions noted.
CC3.2.3	Asset inventory listings of hardware and systems required for the provision of data center hosting services are maintained for review during the annual risk assessment process.	Inquired of the security and compliance analyst regarding the risk assessment procedures to determine that asset inventory listings of hardware and systems required for the provision of data center hosting services were maintained for review during the annual risk assessment process.	No exceptions noted.
		Inspected the asset inventory equipment listings for a sample of IBX data center facilities to determine that asset inventory listings of equipment required for the provision of the data center hosting services was maintained for each facility 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	Documented risk assessment policies and procedures are in place to guide personnel in identifying and analyzing risks including the potential for fraud.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying and analyzing risks including the potential for fraud.	No exceptions noted.
CC3.3.2	A risk assessment is performed on an annual basis that considers the potential for fraud. Risks that are identified are rated using a risk evaluation process and are formally documented for management review.	Inspected the most recent annual IBX threat and risk assessments for a sample of data center facilities to determine that risk assessments were performed during the review period that addressed the potential fraud risks, and that risks were identified using a risk evaluation process and formally documented, along with activities, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Documented policies and procedures are in place to guide personnel in the identification and assessment of relevant changes that could significantly impact the system and services provided.	Inspected the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in the identification and assessment of relevant changes that could significantly impact the system and services provided.	No exceptions noted.
CC3.4.2	A risk assessment is performed on an annual basis that includes consideration for internal and external changes that could significantly impact the system and services provided. Risks that are identified are rated using a risk evaluation process and formally documented, along with mitigation strategies, for management review.	Inspected the most recent annual IBX threat and risk assessments for a sample of data center facilities to determine that risk assessments were performed during the review period that considered that considered the impact of internal and external changes to the system and services provided, and that risks were identified using a risk evaluation process and formally documented, along with activities, for management review.	No exceptions noted.
CC3.4.3	The entity's global information security group monitors the security impact of emerging technologies and threats, and notifies relevant personnel.	Inspected example IT security subscription service e-mail notifications received during the review period to determine that the entity's IT security and compliance groups monitored the security impact of emerging technologies and that the impacts of applicable laws or regulations were considered by senior management.	No exceptions noted.
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal	Inspected the network vulnerability assessment results for a sample of quarters during the review period to determine that a network vulnerability assessment was performed by IT personnel for each quarter sampled.	No exceptions noted.
		Inspected the most recent annual penetration testing report to determine that an external penetration testing for the customer web portal was performed by a third-party vendor during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.2	An internal audit is completed on an annual basis to assess whether the components of internal control are present and operating effectively.	Inspected the internal audit plan and the results of the most recent internal audit to determine that an internal audit was completed during the review period to assess the components of internal control for design and operating effectiveness.	No exceptions noted.
CC4.1.3	Risk treatment activities are documented, tracked, and communicated to those parties responsible for taking corrective action on internal control deficiencies.	Inspected the most recent risk assessment documentation for a sample of IBX data center facilities to determine that risk treatment activities were documented, tracked, and communicated to parties responsible parties for taking corrective action during the period.	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	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal • Remediation plans are proposed and monitored through resolution.	Inspected the network vulnerability assessment results and the corresponding remediation documentation for a sample of quarters during the review period to determine that a network vulnerability assessment was performed by IT personnel for each quarter sampled and that remediation plans were documented and tracked for resolution.	No exceptions noted.
		Inspected the most recent annual penetration testing report and the corresponding remediation documentation to determine that an external penetration testing for the customer web portal was performed by a third-party vendor during the review period and that remediation plans were documented and tracked for resolution.	No exceptions noted.
CC4.2.2	An internal audit is completed on an annual basis to ascertain whether the components of internal control are present and functioning. Issues that are identified are tracked and monitored through resolution.	Inspected the internal audit plan, the results of the most recent internal audit, and the corrective action plan tracker to determine that an internal audit was completed during the review period to assess the components of internal control for design and operating effectiveness; and issues that were identified were tracked and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.3	ISMC meetings are held on a quarterly basis to discuss internal control assessments and deficiencies to ensure that corrective action is taken.	Inspected the corrective action plan tracker and management meeting minutes for a sample of quarters during the review period to determine that ISMC meetings were held during each quarter sampled that included discussion points for internal control assessments, deficiencies, and corrective actions taken.	No exceptions noted.
CC4.2.4	Information security audit and compliance assessments are conducted by an accredited independent third-party assessors on an annual basis. The results of the assessments are reviewed by management.	Inspected the audit reports and compliance documentation obtained for management review as well as the meeting minutes for management reviews performed during the review period to determine that information security audit and compliance assessments were conducted by an accredited independent third-party assessors on an annual basis and results of the assessments were reviewed by management.	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	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to objectives. Mitigation strategies including the selection and development of control activities by assigned risk owners are documented for management review.	Inspected the most recent risk assessment documentation for a sample of IBX data center facilities to determine that annual risk assessments were performed during the review period that considered the identification and assessment of risks relating to objectives and that mitigation strategies included the selection and development of control activities by assigned risk owners were documented for management review.	No exceptions noted.
CC5.1.2	Risk treatment activities are documented, tracked, and communicated to those parties responsible for taking corrective action on internal control deficiencies.	Inspected the most recent risk assessment documentation for a sample of IBX data center facilities to determine that risk treatment activities were documented, tracked, and communicated to parties responsible parties for taking corrective action during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.3	A key controls matrix of applicability is documented and maintained identifies the control activities to support the achievement of objectives along with control justifications and a description of how the control activities are implemented.	Inspected the controls matrix to determine that a key controls matrix was in place that identified the entity's control activities supporting the achievement of objectives including control justifications and a description of how the control activities were implemented.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to objectives. Mitigation strategies including the selection and development of general control activities over technology by assigned risk owners are documented for management review.	Inspected the most recent risk assessment documentation for a sample of IBX data center facilities to determine that annual risk assessments were performed during the review period that considered the identification and assessment of risks relating to objectives and that mitigation strategies included the selection and development of general control activities over technology by assigned risk owners were documented for management review.	No exceptions noted.
CC5.2.2	A key controls matrix is documented and maintained identifies the technology control activities to support the achievement of objectives along with control justifications and a description of how the control activities are implemented.	Inspected the controls matrix to determine that a key controls matrix was in place that identified the entity's technology control activities supporting the achievement of objectives including control justifications and a description of how the control activities were implemented.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of the in-scope systems. These policies and procedures are communicated to internal personnel via the intranet.	Inspected the security policy documentation maintained on the internal intranet to determine that documented policies were in place to guide personnel in the entity's security and availability commitments and the associated system requirements, and that the policies were communicated to internal personnel via the company Intranet.	No exceptions noted.
CC5.3.2	Employee sanction policies are documented to communicate consequences for disciplinary actions, up to and including termination, for violations to company policies and the code of conduct.	Inspected the employee sanction policies to determine that documented employee sanction policies were in place to communicate consequences for disciplinary action, up to an including termination, for violation to company policies and the code of conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	Employees are required to complete new hire security awareness training and annual security awareness training thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training materials and completion records for a sample of employees hired during the review period to determine that new hire security awareness training was completed for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
		Inspected the security awareness training materials and completion records for a sample of existing employee to determine that security awareness training was completed during the review period for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	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	Access to the in scope systems requires users to authenticate via a user account and password. The network domain is configured to enforce predefined user account and minimum password requirements.	Observed the login procedures for a sample of IBX data center systems with the assistance of site security and engineering personnel to determine that users were required to authenticate via a user account and password for each system sampled.	No exceptions noted.
		Inspected the user access listings and authentication configurations for a sample of applications, network operating systems, and devices to determine that users were required to authenticate via a user account and password for each system sampled.	No exceptions noted.
		Inspected the user account and password group policies for the network domain to determine that the network domain was configured to enforce predefined user account and minimum password requirements.	No exceptions noted.
CC6.1.2	VPN gateways are utilized to establish secure connections and are configured to enforce two-factor authentication requirements for access to the corporate network.	Inspected the user authentication and encryption policy configurations for a sample of VPN gateways to determine that VPN gateways were utilized to establish secure connections to the corporate network and were configured to enforce two-factor authentication requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in scope systems.	Observed the user account and role assignment listings for a sample of IBX data center systems with the assistance of site security and engineering personnel to determine that predefined security groups were utilized, where applicable, to assign role-based access privileges for each system sampled.	No exceptions noted.
		Inspected the user account and role assignment listings for a sample of in scope applications, network operating systems, and devices to determine that predefined security groups were utilized, where applicable, to assign role-based access privileges for each system sampled.	No exceptions noted.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Observed the administrator user account listings for a sample of IBX data center systems with the assistance of site security and engineering personnel to determine that administrative access privileges were restricted to user account accessible by authorized personnel for each system sampled.	No exceptions noted.
		Inspected the administrator user account listings for a sample of in scope applications, network operating systems, and devices with the assistance of corporate IT security personnel to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for each system sampled.	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	Procedures exist and are followed to establish new user access privileges to production systems.	Inspected the user access request tracking documentation for a sample of employees hired during the review period to determine that procedures existed and were followed to establish new user access privileges to production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.2	A termination ticket is completed, and network access is revoked for employees as a component of the employee termination process.	Inspected the termination tracking documentation and network user account listing for a sample of employees terminated during the review period to determine that a termination ticket was completed, and network access was revoked for each 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	Procedures exist and are followed to establish new user access privileges to production systems.	Inspected the user access request tracking documentation for a sample of employees hired during the review period to determine that procedures existed and were followed to establish new user access privileges to production systems.	No exceptions noted.
CC6.3.2	A termination ticket is completed, and network access is revoked for employees as a component of the employee termination process.	Inspected the termination tracking documentation and network user account listing for a sample of employees terminated during the review period to determine that a termination ticket was completed, and network access was revoked for each employee sampled.	No exceptions noted.
CC6.3.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in scope systems.	Observed the user account and role assignment listings for a sample of IBX data center systems with the assistance of site security and engineering personnel to determine that predefined security groups were utilized, where applicable, to assign role-based access privileges for each system sampled.	No exceptions noted.
		Inspected the user account and role assignment listings for a sample of in scope applications, network operating systems, and devices to determine that predefined security groups were utilized, where applicable, to assign role-based access privileges for each system sampled.	No exceptions noted.
CC6.3.4	Administrative access privileges to the in scope systems are restricted to user accounts accessible by authorized personnel.	Observed the administrator user account listings for a sample of IBX data center systems with the assistance of site security and engineering personnel to determine that administrative access privileges were restricted to user account accessible by authorized personnel for each system sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the administrator user account listings for a sample of in scope applications, network operating systems, and devices with the assistance of corporate IT security personnel to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for each system sampled.	No exceptions noted.
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	Physical access control systems are in place to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorized individuals.	Observed the physical access control systems at each facility to determine that physical access controls were in place that restricted access that included the following: • Badge access control system in place at the perimeter and within the facilities • Two-factor authentication system required access to the data centers • Visitor logs recorded visitor access to the corporate facility and the data centers • Visitors were required to wear visitor badges while onsite and the badges were distinguishable from employee badges • Visitors required an escort at all times	No exceptions noted.
CC6.4.2	Procedures exist and are followed to established and make changes to physical access privileges for customers.	Observed the change tracking documentation for a sample of customer physical access change requests received during the review period to determine that procedures were followed to establish and make changes to physical access privileges for customers to each facility.	No exceptions noted.
CC6.4.3	Procedures exist and are followed to established and make changes to physical access privileges for employees.	Inspected the access request tracking documentation for a sample of employees hired during the review period to determine that procedures existed and were followed to grant physical access privileges for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access termination tracking documentation for a sample of employees terminated during the review period to determine that procedures existed and were followed to revoke physical access privileges for each employee sampled.	No exceptions noted.
CC6.4.4	Security personnel review a government issued ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to the facility.	Observed the physical access procedures at the data center facilities to determine that security personnel reviewed a government issues ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to each facility.	No exceptions noted.
CC6.4.5	Visitors are required to sign a visitor log upon entering the facility, and be escorted by an authorized employee when accessing the facility.	Observed the visitor access procedures at the data center facilities to determine that visitors were required to sign a visitor log upon entry and be escorted by an authorized employee when accessing each facility.	No exceptions noted.
CC6.4.6	A proximity card system and / or a biometric reader and PIN are required to restrict access to the facility.	Observed the physical access control systems in place at the data center facilities to determine that a proximity card system and / or a biometric reader and PIN were in place to restrict access to each facility.	No exceptions noted.
CC6.4.7	Physical access system logs are recorded and maintained for a minimum of six months.	Observed the historical physical access system logs maintained for the data center facilities to determine that physical access system logs were available for at least six months from the date of observation for each facility.	No exceptions noted.
		Inspected the historical physical access control and visitor management systems logs maintained for a sample of data center facilities to determine that physical access system logs were recorded and retained for at least six months from the date of inspections for each facility.	No exceptions noted.
CC6.4.8	Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.	Observed the monitoring procedures at the data center facilities to determine that monitoring of physical activity was performed through the use of onsite security monitoring and/or digital surveillance cameras at each facility.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security monitoring shift schedules for a sample of data center facilities and months during the review period to determine that onsite and offsite security personnel were scheduled 24x7 to monitor each facility during each month sampled.	No exceptions noted.
CC6.4.9	Surveillance camera logs are recorded and maintained for a minimum of 30 days.	Observed the historical surveillance camera logs maintained for the data center facilities to determine that surveillance camera footage was available for review at least 30 days from the date of observation for each facility.	No exceptions noted.
		Inspected the historical surveillance camera logs for a sample of data center facilities to determine that surveillance camera footage was available for review at least 30 days from the date of observation for each facility sampled.	No exceptions noted.
CC6.4.10	Each customer has a defined space within the data center that is physically secured within a locked cage and / or cabinet.	Observed the colocation space at the data center facilities to determine that customers had defined space within the data center that were physically secured within a locked cage and / or cabinet for each facility.	No exceptions noted.
CC6.4.11	The data center floor does not have any windows leading to the exterior of the building. In case due to the existing infrastructure there are windows leading to the exterior then they need to be locked from the inside or access controlled.	Observed the colocation space at the data center facilities to determine that the data center floor did not have any windows leading to the exterior of the building or in the case due to the existing infrastructure there were windows leading to the exterior, those windows were locked from the inside or access controlled for each facility.	No exceptions noted.
CC6.4.12	Physical user access reviews are performed at least quarterly to help ensure that physical access to the data center facilities is restricted authorized personnel.	Inspected the physical user access review documentation for a sample IBX data centers and quarters during the review period to determine that physical user access reviews were performed for each data center and quarter sampled.	No exceptions noted.
	Digital Realty Trust is responsible for ensuring that physical access to the Dallas 10 (DA10) data center facility (including colocation space, backup media storage and other sensitive locations as well as sensitive system component within this locations) is restricted authorized personnel.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Asset removal and disposal policies are in place to guide personnel in the disposal of assets to ensure data and software was unrecoverable prior to retiring a physical asset.	Inspected the asset disposal policies to determine that asset removal and disposal policies were in place to guide personnel in the disposal of assets to ensure data and software was unrecoverable prior to retiring a physical asset.	No exceptions noted.
CC6.5.2	Media containing sensitive data is securely wiped or destroyed prior to retiring a physical asset.	Inspected the certificates of destruction for a sample of hard drives containing sensitive data retired during the review period to determine that the physical assets containing sensitive data were securely destroyed by a third-party specialist for asset retirement.	No exceptions noted.
	Digital Realty Trust is responsible for ensuring that physical access to the Dallas 10 (DA10) data center facility (including colocation space, backup media storage and other sensitive locations as well as sensitive system component within this locations) is restricted authorized personnel.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Inspected the global firewall rulesets maintained within the centralized network security management utility to determine that firewall systems were in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.6.2	An IDS is utilized to monitor and analyze network traffic and is configured to alert IT security and NOC personnel for possible or actual security breach events.	Inquired of the IT security personnel regarding the monitoring to determine that IT security and NOC personnel were available to monitor and address system alerts for possible or actual security breach events.	No exceptions noted.
		Inspected the threat detection and alerting parameters configured within the IDS as well as example e-mail alert notifications generated by the system during the review period to determine that an IDS was utilized to monitor and analyze network traffic and configured to alert IT security and NOC personnel for possible or actual security breach events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.3	Encrypted VPNs are required to remotely access the corporate network and are configured to enforce two-factor authentication.	Inspected the VPN encryption and authentication configurations for sample of VPN gateways to determine that encrypted VPNs were required to remotely access the corporate network and were con figured to enforce two-factor authentication.	No exceptions noted.
CC6.6.4	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal	Inspected the network vulnerability assessment results for a sample of quarters during the review period to determine that a network vulnerability assessment was performed by IT personnel for each quarter sampled.	No exceptions noted.
		Inspected the most recent annual penetration testing report to determine that an external penetration testing for the customer web portal was performed by a third-party vendor during the review period.	No exceptions noted.
CC6.6.5	Equinix Customer Portal web servers utilize transport layer security (TLS) 1.2 encryption for web communication sessions.	Inspected digital certificates for the Equinix Customer Portal web servers determine that the web servers utilized TLS 1.2 encryption for web communication sessions.	No exceptions noted.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policies to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Equinix Customer Portal web servers utilize TLS 1.2 encryption for web communication sessions.	Inspected digital certificates for the Equinix Customer Portal web servers determine that the web servers utilized TLS 1.2 encryption for web communication sessions.	No exceptions noted.
CC6.7.3	Encrypted VPNs are required to remotely access the corporate network and are configured to enforce two-factor authentication.	Inspected the VPN encryption and authentication configurations for sample of VPN gateways to determine that encrypted VPNs were required to remotely access the corporate network and were con figured to enforce two-factor authentication.	No exceptions noted.

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	An enterprise antivirus server is configured with next generation antivirus/antimalware software for endpoint protection of registered production Windows servers and workstations.	Inspected the enterprise antivirus software configurations and registered client list to determine that enterprise antivirus server was configured with next generation antivirus/antimalware software for endpoint protection of registered production Windows servers and workstations.	No exceptions noted.
CC6.8.2	A SIEM application is utilized to monitor and log certain security events for the in-scope systems and is configured to alert IT personnel when predefined conditions are met.	Inspected the SIEM application configurations and example e-mail alerts generated during the review period to determine that a SIEM application was in place to monitor and log certain security event for the in-scope systems and configured to alert IT personnel when predefined conditions were met.	No exceptions noted.
CC6.8.3	An IDS is utilized to monitor and analyze network traffic and is configured to alert IT security and NOC personnel for possible or actual security breach events.	Inquired of the IT security personnel regarding the monitoring to determine that IT security and NOC personnel were available to monitor and address system alerts for possible or actual security breach events.	No exceptions noted.
		Inspected the threat detection and alerting parameters configured within the IDS as well as example e-mail alert notifications generated by the system during the review period to determine that an IDS was utilized to monitor and analyze network traffic and configured to alert IT security and NOC personnel for possible or actual security breach events.	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	A SIEM application is utilized to monitor and log certain security events for the in scope systems and is configured to alert IT personnel when predefined conditions are met.	Inspected the SIEM application configurations and example e-mail alerts generated during the review period to determine that a SIEM application was in place to monitor and log certain security event for the in scope systems and configured to alert IT personnel when predefined conditions were met.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal	Inspected the network vulnerability assessment results for a sample of quarters during the review period to determine that a network vulnerability assessment was performed by IT personnel for each quarter sampled.	No exceptions noted.
		Inspected the most recent annual penetration testing report to determine that an external penetration testing for the customer web portal was performed by a third-party vendor during the review period.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	A SIEM application is utilized to monitor and log certain security events for the in scope systems and is configured to alert IT personnel when predefined conditions are met.	Inspected the SIEM application configurations and example e-mail alerts generated during the review period to determine that a SIEM application was in place to monitor and log certain security event for the in scope systems and configured to alert IT personnel when predefined conditions were met.	No exceptions noted.
CC7.2.2	An IDS is utilized to monitor and analyze network traffic and is configured to alert IT security and NOC personnel for possible or actual security breach events.	Inquired of the IT security personnel regarding the monitoring to determine that IT security and NOC personnel were available to monitor and address system alerts for possible or actual security breach events.	No exceptions noted.
		Inspected the threat detection and alerting parameters configured within the IDS as well as example e-mail alert notifications generated by the system during the review period to determine that an IDS was utilized to monitor and analyze network traffic and configured to alert IT security and NOC personnel for possible or actual security breach events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.3	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: • Quarterly network vulnerability assessments • Annual external penetration testing for the customer web portal Remediation plans are proposed and monitored through resolution.	Inspected the network vulnerability assessment results and the corresponding remediation documentation for a sample of quarters during the review period to determine that a network vulnerability assessment was performed by IT personnel for each quarter sampled and that remediation plans were documented and tracked for resolution.	No exceptions noted.
		Inspected the most recent annual penetration testing report and the corresponding remediation documentation to determine that an external penetration testing for the customer web portal was performed by a third-party vendor during the review period and that remediation plans were documented and tracked for resolution.	No exceptions noted.
CC7.2.4	Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.	Observed the monitoring procedures at the data center facilities to determine that monitoring of physical activity was performed through the use of onsite security monitoring and/or digital surveillance cameras at each facility.	No exceptions noted.
		Inspected the security monitoring shift schedules for a sample of data center facilities and months during the review period to determine that onsite and offsite security personnel were scheduled 24x7 to monitor each facility during each month sampled.	No exceptions noted.
CC7.2.5	A BMS is used to monitor the critical data center facility equipment and alert personnel of any potential issues. BMS systems are monitored 24x7 by onsite or on call facilities engineers.	Observed the data center facility engineer staffing schedules for a sample of data center facilities and months during the review period to determine that onsite or on call facilities engineers were scheduled 24x7 to monitor each facility during each month sampled.	No exceptions noted.
		Inspected the BMS monitoring dashboard and example alert log notifications generated during the review period for a sample of data center facilities to determine that a BMS was used to monitor the critical facility equipment and alert personnel when potential issues were identified for each facility sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Incident response procedures are in place that outline the response procedures to security events including lessons learned.	Inspected the incident response procedures to determine that incident response procedures were in place that outlined the response procedures to security events including lessons learned.	No exceptions noted.
CC7.3.2	Procedures are in place requiring that incidents resulting in a change to the system follow a standard change control process.	Inquired of the compliance specialist regarding security incident management procedures to determine that incidents requiring a change to the system followed the standard control process.	No exceptions noted.
		Inspected the incident management procedures to determine that procedures were in place requiring that incident resulting in a change to the system follow a standard change control process.	No exceptions noted.
CC7.3.3	An enterprise ticketing system is utilized to document and track system security and availability incidents through resolution.	Inspected the listing of incident tickets logged in the ticketing system and the incident ticket details for a sample of incidents during the review period to determine that an enterprise ticketing system was utilized to document and track system security and availability incidents through resolution during the review period.	No exceptions noted.
CC7.3.4	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items.	Inspected the root cause analysis documentation for a sample of incident reported during the review period to determine that a root cause analysis was performed that addressed impact analysis, resolution, lessons learned, and/or action items for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Documented incident response procedures are in place to guide personnel in the following steps required for the incident response process: • Roles and responsibilities • Incident identification, investigation, and triage • Communication protocols for affected parties • Remediation (containment, eradication, and recovery) • Post incident activities (restoration and lessons learned)	Inspected the incident response policies and procedures to determine that documented incident response procedures were in place to guide personnel in the following steps required for the incident response process: • Roles and responsibilities • Incident identification, investigation, and triage • Communication protocols for affected parties • Remediation (containment, eradication, and recovery) • Post incident activities (restoration and lessons learned)	No exceptions noted.
CC7.4.2	An enterprise ticketing system is utilized to document and track system security and availability incidents through resolution.	Inspected the listing of incident tickets logged in the ticketing system and the incident ticket details for a sample of incidents during the review period to determine that an enterprise ticketing system was utilized to document and track system security and availability incidents through resolution during the review period.	No exceptions noted.
CC7.4.3	Incident response plan testing is performed on an annual basis at each site using simulated security incidents to determine the incident response effectiveness and documents the results.	Inspected the most recent incident response plan testing results for a sample of IBX data center facilities to determine that incident response plan testing was performed during the review using simulated security incidents and the results documented for each facility sampled.	No exceptions noted.
CC7.4.4	Data center facility incidents and corrective measures are reported on monthly for management review.	Inspected the security KPI reports for a sample of IBX data center facilities and months during the review period to determine that data center facility KPI reports addressing incidents and corrective measures were reported for management review for each facility and month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response procedures are in place to guide personnel in the following steps required for the incident response process: • Roles and responsibilities • Incident identification, investigation, and triage • Communication protocols for affected parties • Remediation (containment, eradication, and recovery) • Post incident activities (restoration and lessons learned)	Inspected the incident response policies and procedures to determine that documented incident response procedures were in place to guide personnel in the following steps required for the incident response process: • Roles and responsibilities • Incident identification, investigation, and triage • Communication protocols for affected parties • Remediation (containment, eradication, and recovery) • Post incident activities (restoration and lessons learned)	No exceptions noted.
CC7.5.2	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items.	Inspected the root cause analysis documentation for a sample of incident reported during the review period to determine that a root cause analysis was performed that addressed impact analysis, resolution, lessons learned, and/or action items for each incident sampled.	No exceptions noted.
CC7.5.3	Incident response plan testing is performed on an annual basis at each site using simulated security incidents to determine the incident response effectiveness and documents the results.	Inspected the results of the most recent annual incident response plan testing for a sample of IBX data center facilities to determine that incident response plan testing was performed during the review using simulated security incidents and the results documented for each facility sampled.	No exceptions noted.
CC7.5.4	A crisis management team meeting is held on an annual basis to assess the team's ability to effectively response to cyber incidents.	Inspected the current global crisis management plan and most recent annual crisis management team meeting agenda and assessment report to determine that a crisis management team meeting was held during the review period that included assessment activities related to the team's ability to effectively respond to cyber incidents. .	No exceptions noted.
CC7.5.5	Procedures are in place requiring that incidents resulting in a change to the system follow a standard change control process.	Inspected the incident management procedures to determine that procedures were in place requiring that incident resulting in a change to the system follow a standard change control process.	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	Documented change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes.	Inspected the change management policies and procedures to determine that documented change management policies and procedures were in place to guide personnel in the request, documentation, testing, and approval of changes.	No exceptions noted.
CC8.1.2	Changes made to in-scope systems are authorized, tested if applicable, and approved prior to implementation.	Inspected the change documentation for a sample of application and infrastructure changes implemented during the review period to determine that each change sampled was authorized, tested when applicable, and approved.	No exceptions noted.
CC8.1.3	A ticketing system is utilized to centrally document and track configuration and maintenance activities.	Inspected the change request tickets for a sample of configurations and maintenance changed during the review period to determine that a ticket system was utilized to document and track configuration and maintenance activities.	No exceptions noted.
CC8.1.4	The production environment is logically segmented from the test environments.	Inspected the network IP address configurations to determine that the production environment was logically segmented from the test environments.	No exceptions noted.
CC8.1.5	A change review meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the change review meeting documentation for a sample of weeks during the review period to determine that a change management meeting was held to discuss and communicate the ongoing and upcoming projects that affected the system for each week sampled.	No exceptions noted.
CC8.1.6	Access privileges to promote changes into the production environment is restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listings for a sample of in scope applications, network operating systems, and devices with the assistance of corporate IT security personnel to determine that administrative access privileges were restricted to user accounts accessible by authorized personnel for each system sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in the identification, selection, and development of risk management activities for risks arising from potential business disruptions.	Inspected the risk management policies and procedures and the IBX business recovery plans to determine that documented policies and procedures were in place to guide personnel in the identification, selection, and development of risk management activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.2	A risk assessment is performed on an annual basis that considers risks arising from potential business disruptions. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation for a sample of IBX data center facilities to determine that annual risk assessments were performed that considered risks arising from potential business disruptions and that risks identified were rated using a risk evaluation process and formally documented, along with mitigation strategies, for management review.	No exceptions noted.
CC9.1.3	Insurance is in place for the data center locations and equipment.	Inspected the certificate of property insurance for the data center facilities to determine that the data center locations and equipment were covered under an active insurance policy during the review period.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	A risk assessment is performed on an annual basis that considers risks associated with third-party providers accessing the data center facilities. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation for a sample of IBX data center facilities to determine that risk assessments were performed during the review period that considered risks associated with third-party providers accessing the data center facilities and risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review.	No exceptions noted.
CC9.2.2	Signed agreements addressing information security and confidentiality obligations are required to be in place with third-party providers prior to sharing restricted information with the provider or providing access to data center facilities.	Inspected the service level agreements for a sample of the third-party providers to determine that signed agreements addressed information security and confidentiality obligations were required to be in place with third-party providers prior to the entity doing business the providers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.3	Operations and compliance personnel perform periodic third-party provider performance review activities to help ensure that the providers are in compliance with the organization's requirements.	Inspected the vendor management questionnaires and supplier performance review documentation for third-party provider performance review activities performed during the review period to determine that periodic third-party performance review activities were performed to help ensure the third-party providers were compliant with the organization's requirements.	No exceptions noted.
		Inspected the KPI and scorecard summary reports for a sample of months and data center facilities that employed onsite security personnel to determine that security team KPIs were reported and reviewed for compliance with the organization's requirements for each month and facility 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	System monitoring applications are configured to monitor the in-scope systems capacity levels and alert operations personnel when predefined thresholds have been met.	Inspected the enterprise monitoring application configurations and example alert notifications generated during the review period to determine that enterprise monitoring applications were configured to monitor in-scope network systems capacity levels and alert operations personnel when predefined thresholds were met.	No exceptions noted.
		Inspected the BMS monitoring dashboard and example alert log notifications generated during the review period for a sample of data center facilities to determine that a BMS was used to monitor the critical facility equipment and alert personnel when potential issues were identified for each facility sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.2	Resource utilization incidents are tracked within a ticketing system and reported to IT operations personnel on a monthly basis for review and response to capacity management needs.	Inspected the resource utilization reporting documentation and corresponding ticket tracker details for a sample of months during the review period to determine that resource utilization was tracked within a ticketing system and reported to IT operation personnel for review for each month 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	Fire detection and suppression equipment is in place at each facility.	Observed the fire detection and suppression equipment at the data center facilities to determine that fire detection and suppression equipment was in place at each facility.	No exceptions noted.
A1.2.2	Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.	Observed the fire detection and suppression equipment maintenance documentation onsite with the assistance of facilities personnel at the data center facilities to determine that scheduled maintenance procedures were performed to help ensure that fire detection and suppression equipment was working properly during the review period at each facility.	No exceptions noted.
		Inspected the most recent fire detection and suppression equipment preventative maintenance reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed for the fire detection and suppression equipment during the review period for each facility sampled.	No exceptions noted.
A1.2.3	Power management equipment is in place for each facility.	Observed the power management equipment at the data center facilities to determine that power management equipment was in place at each facility.	No exceptions noted.
A1.2.4	Scheduled maintenance procedures are performed to test and confirm the operation of the power management systems.	Observed the power management system maintenance documentation onsite with the assistance of facilities personnel at the data center facilities to determine that scheduled maintenance procedures were performed to test and confirm the operation of the power management systems during the review period at each facility.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent UPS and generator preventative maintenance reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed for the power management systems during the review period for each facility sampled.	No exceptions noted.
A1.2.5	Air conditioning and ventilation equipment is in place at each facility to ensure that humidity levels and the required temperature are maintained.	Observed the HVAC equipment at the data center facilities to determine that air conditioning and ventilation equipment was in place at each facility.	No exceptions noted.
A1.2.6	Scheduled maintenance procedures are performed to ensure that the HVAC equipment and temperature and water detection sensors are working properly.	Observed the HVAC equipment maintenance documentation onsite with the assistance of facilities personnel at the data center facilities to determine that scheduled maintenance procedures were performed to help ensure that the HVAC equipment and temperature and water detection sensors were working properly during the review period at each facility.	No exceptions noted.
		Inspected the most recent HVAC equipment preventative maintenance reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed for the HVAC equipment during the review period for each IBX facility sampled.	No exceptions noted.
A1.2.7	Internal and external monitoring of environmental systems activity is performed through the use of BMS and 24x7 monitoring by facility engineers.	Observed the facility monitoring procedures at the data center facilities to determine that each facility was monitored by facilities engineers during standard business hours.	No exceptions noted.
		Observed the data center facility engineer staffing schedules for a sample of data center facilities and months during the review period to determine that onsite or on call facilities engineers were scheduled 24x7 to monitor each facility during each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.8	Backup systems are in place to perform scheduled backups of production data at predefined times.	Inspected the backup utility configurations, image backup archive, and example backup logs generated during the review period for a sample of data center systems to determine that backup systems were in place to perform scheduled backups of production data at predefined times.	No exceptions noted.
A1.2.9	Emergency procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the IBX emergency policies and procedures and the security staff procedures to determine to determine that emergency procedures were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected the IBX business recovery plans for a sample of in-scope IBX data center facilities to determine that a business recovery plan was in place to protect against disruptions caused by an unexpected event for each facility sampled.	No exceptions noted.
	Digital Realty Trust is responsible for the environmental protection controls design, development, implementation, operations, maintenance, and monitoring to meet availability commitments and requirements at the Chicago 4 (CH4) data center facility.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Scheduled maintenance procedures are performed on environmental systems to ensure system recovery.	Inspected the environmental systems preventative maintenance reports for a sample of IBX data center facilities to determine that scheduled maintenance procedures were performed on environmental systems during the review period at each facility sampled.	No exceptions noted.
A1.3.2	Disaster recovery testing is performed for each site on an annual basis to ensure that the site can operate in the event of a disaster.	Inspected the most recent 'pull the plug' testing results for a sample of IBX data center facilities to determine that disaster recovery testing was performed during the review period for each facility sampled.	No exceptions noted.