EQUINIX

EQUINIX, INC.

SOC 2 REPORT

FOR

GLOBAL DATA CENTER HOUSING SERVICES

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

NOVEMBER 1, 2023, TO OCTOBER 31, 2024

Attestation and Compliance Services

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

TABLE OF CONTENTS

SECTION 1

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 Global Data Center Housing Services system, in Section 3, throughout the period November 1, 2023, to October 31, 2024, (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, 2023, to October 31, 2024, 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 various subservice organizations for environmental protection control services at the Chicago 4 (CH4), Seoul 1 (SL1), Dublin 1 (DB1), Dubai 2 (DX2) and Abu Dhabi 1 (AD1). 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 organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Equinix" is presented by Equinix management to provide additional information and is not a part of the description. Information about Equinix's management's responses to exceptions noted and Equinix's Global Data Privacy Positioning Statement has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Equinix's service commitments and system requirements based on the applicable trust services criteria.

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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were

achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

Service Auditor's Independence and Quality Control

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

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

Inherent Limitations

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

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

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

Description of Test of Controls

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

Opinion

In our opinion, in all material respects:

a. the description presents Equinix's Global Data Center Housing Services system that was designed and implemented throughout the period November 1, 2023, to October 31, 2024, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period November 1, 2023, to October 31, 2024, 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, 2023, to October 31, 2024, 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 Global Data Center Housing Services system during some or all of the period of November 1, 2023, to October 31, 2024, business partners of Equinix subject to risks arising from interactions with the Global Data Center Housing 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
November 29, 2024

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Equinix's Global Data Center Housing Services system, in Section 3, throughout the period November 1, 2023, to October 31, 2024, (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 Global Data Center Housing 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 various subservice organizations for environmental protection control services at the Chicago 4 (CH4), Seoul 1 (SL1) Dublin 1 (DB1), Dubai 2 (DX2) and Abu Dhabi 1 (AD1) IBX data centers. 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 organizations.

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

a. the description presents Equinix's Global Data Center Housing Services system that was designed and implemented throughout the period November 1, 2023, to October 31, 2024, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period November 1, 2023, to October 31, 2024, 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, 2023, to October 31, 2024, 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.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Overview

Equinix (Nasdaq: EQIX) is the world's digital infrastructure company. Digital leaders harness Equinix's trusted platform to bring together and interconnect foundational infrastructure at software speed. Equinix enables organizations to access places, partners and possibilities to scale with agility, speed the launch of digital services, while supporting their sustainability goals.

Description of Services Provided

Equinix provides data center housing services at the 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 housing 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 housing 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 housing services, and the financial, operational, and compliance requirements that Equinix has established for the services. The data center housing 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 thresholds for temperature, humidity levels, and 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 Housing Services system.

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

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

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

The scope of the review includes the data center facilities located in the metropolitan areas listed below. Additionally, the support and management functions of the Tampa, Florida, field office (TPFO) supporting the data center housing services provided at the Americas (AMER) sites was included within the scope of the review.
The following IBX data centers and sites were included within the scope of the review:

Region	Country	Metro	Site
Americas (AMER)	United States of America (USA)	Atlanta	AT1, AT4
		Boston	BO2
		Chicago	CH1, CH2, CH3, CH4^, CH7
		Culpepper	CU1, CU2, CU3, CU4
		Dallas	DA1, DA2, DA3, DA4, DA6, DA7, DA9, DA11
		Denver	DE1, DE2
		Houston	HO1
		Los Angeles	LA1, LA2, LA3, LA4, LA7
		Miami	MI1, MI2, MI3, MI6
		New York	NY1, NY2, NY4, NY5, NY6, NY7, NY9, NY11, NY13
		Philadelphia	PH1
		Seattle	SE2, SE3, SE4

Region	Country	Metro	Site
Americas (AMER)	United States of America (USA)	Silicon Valley	SV1, SV2, SV3, SV4, SV5, SV8, SV10, SV11, SV12x, SV14, SV15, SV16
		Tampa	TPFO
		Washington D.C.	DC1, DC2, DC3, DC4, DC5, DC6, DC7, DC10, DC11, DC12, DC13, DC14, DC15, DC16, DC21, DC97
	Brazil	Rio De Janeiro	RJ1, RJ2
		São Paulo	SP1, SP2, SP3, SP4, SP5x
	Canada	Calgary	CL1, CL2, CL3
		Kamloops	KA1
		Montreal	MT1, MT2
		Ottawa	OT1
		Saint John	SJ1
		Toronto	TR1, TR2, TR5, TR6, TR7
		Vancouver	VA1
		Winnipeg	WI1
	Chile	Santiago	ST1, ST2, ST3, ST4
	Colombia	Bogota	BG1, BG2
	Mexico	Mexico City	MX1, MX2
		Monterrey	MO1
	Peru	Lima	LM1
Europe, Middle East, and Africa (EMEA)	Bulgaria	Sofia	SO1, SO2
	Finland	Helsinki	HE3, HE4, HE5, HE6, HE7
	France	Paris	PA2, PA3, PA4, PA5, PA6, PA7, PA8x, PA9x, PA10, PA13x
		Bordeaux	BX1
	Germany	Dusseldorf	DU1
		Frankfurt	FR2, FR4, FR5, FR6, FR7, FR8, FR9x, FR11x, FR13
		Hamburg	HH1
		Munich	MU1, MU3, MU4
	Ireland	Dublin	DB1^, DB2, DB3, DB4, DB5x, DB6x **Note1**
	Italy	Milan	ML2, ML3, ML5, ML7x **Note1**
		Genoa	GN1
	Netherlands	Amsterdam	AM1, AM2, AM3, AM4, AM5, AM6, AM7, AM8, AM11
		Enschede	EN1
		Zwolle	ZW1
	Oman	Muscat	MC1
	Poland	Warsaw	WA1, WA2, WA3, WA4x **Note1**

Region	Country	Metro	Site
Europe, Middle East, and Africa (EMEA)	Portugal	Lisbon	LS1
	Spain	Barcelona	BA1
		Madrid	MD1, MD2, MD3x [Note1], MD6
	Sweden	Stockholm	SK1, SK2, SK3
	Switzerland	Geneva	GV1, GV2
		Zurich	ZH2, ZH4, ZH5
	Turkey	Istanbul	IL2
	UAE	Abu Dhabi	AD1^
		Dubai	DX1, DX2^, DX3
	United Kingdom	London	LD3, LD4, LD5, LD6, LD7, LD8, LD9, LD10, LD11x, LD13x
		Manchester	MA1, MA3, MA4, MA5
Asia-Pacific (APAC)	Australia	Adelaide	AE1
		Brisbane	BR1
		Canberra	CA1
		Melbourne	ME1, ME2, ME4, ME5
		Perth	PE1, PE2, PE3,
		Sydney	SY1, SY2, SY3, SY4, SY5, SY6, SY7, SY9x
	China	Shanghai	SH2, SH3, SH5, SH6
		Hong Kong	HK1, HK2, HK3, HK4, HK5
	India	Mumbai	MB1, MB2, MB4
	Japan	Osaka	OS1, OS2x, OS3, OS4x
		Tokyo	TY1, TY2, TY3, TY4, TY5, TY6, TY7, TY8, TY9, TY10, TY11, TY12x, TY13x
	South Korea	Seoul	SL1^, SL2x, SL4
	Malaysia	Johor	JH1
		Kuala Lumpur	KL1
	Singapore	Singapore	SG1, SG2, SG3, SG4, SG5

^Physical Security only; the facility environmental security controls at Chicago 4 (CH4), Seoul 1 (SL1), Dublin 1 (DB1), Dubai 2 (DX2) and Abu Dhabi 1 (AD1) IBX data centers are provided by Digital Realty Trust, Inc. (Digital Realty), Samsung SDS Co. Ltd. (Samsung SDS), BT Communications Ireland Limited (BT Communications Ireland), and Khazna Data Center Limited (Khazna), respectively, and were not included within the scope of this examination.

[Note1]The IBX data center is a new site that opened and became fully operational during the reporting period. Therefore, the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Global Data Center Housing Services system were examined at the following IBX data center facilities for the periods specified as follows:

- Dublin 6 (DB6x) IBX data center facility for the period May 1, 2024, to October 31, 2024
- Warsaw 4 (WA4x) IBX data center facility for the period May 1, 2024, to October 31, 2024

- Madrid 3 (MD3x) IBX data center facility for the period May 1, 2024, to October 31, 2024
- Milan 7 (ML7x) IBX data center facility for the period December 1, 2023, to October 31, 2024

Infrastructure and Software

Equinix's Global Data Center Housing 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 servers and virtual machines (VMs) running Microsoft Windows and Red Hat Enterprise Linux operating systems.

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

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 IBX data center facility) used to restrict IBX 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	IBX 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 IBX data centers 24 hours per day; CCTV cameras are positioned throughout the IBX data centers to monitor and track the activity of any person while inside and outside of the IBX data centers.		
Building Management System (BMS) (various platforms – varies by region / location)	Building management system used to monitor environmental controls and alert IBX data center personnel to potential issues within the IBX data center, including critical electrical components, power management equipment, heating, ventilation, and air-conditioning (HVAC) equipment, and fire detection and suppression equipment.		
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.		
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.		

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System**	**Physical Location**
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 IBX 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)
Microsoft Active Directory (AD)	Directory services used to manage user accounts, access, and authentication requirements.	Windows	
Firewalls, zero trust platform, routers, and switches	Corporate IT managed network devices and systems utilized to restrict, filter, and route traffic for Equinix's corporate network; zero trust platform for secure remote network access (Zero Trust Exchange) used to facilitate secure connectivity.	Palo Alto / Juniper / Cisco / Opengear / Avocent / Zscaler	
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 / IBX Data Center Facilities

As noted in the Subservice Organizations section below, the environmental protection system control systems for CH4, SL1, DB1, DX2 and AD1 are hosted on infrastructure owned by Digital Realty Trust (CH4), Samsung SDS (SL1), BT Communications Ireland (DB1) and Khazna (DX2 and AD1). The Global Data Center Housing Services system are limited to the services and related infrastructure maintained by Equinix and does not include Digital Realty, Samsung SDS, BT Communications Ireland, or Khazna, user entity systems, or the Internet connectivity utilized for accessing user entity environments.

People

Equinix has IBX data centers across AMER, APAC, and EMEA 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 AMER; APAC, and EMEA.

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

IBX Data Center Colocation Services

Equinix's IBX data centers are customizable to support the unique requirements of their customers' business. The sites offer reliability, redundancy, security, customization, power, and cooling availability to meet the requirements of their customers.

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 IBX data center facility, including customer cage areas. Exterior walls may incorporate additional security measures, such as reinforced concrete, electric fencing, 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. Exterior perimeter walls, doors, and windows, and the main interior entry door to the colocation floor, are constructed of materials that conform to standards recommended by Equinix security consultants.

All areas of the IBX 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 IBX data center 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. 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 and/or monitored on a 24x7 basis by professional security staff, 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 rounds of the IBX. Doors, including cages, are secured with biometric readers or proximity card readers. Each cage door has an auto lock mechanism that triggers once the door is closed. If the door is not opened an auto re-lock will trigger after 10 seconds. For shared cages, there are locks on the cabinets. Security systems have dedicated uninterruptible power supply (UPS) systems and standby emergency power (generator) support.

The AE1, BR1, DE1, HE3, HE5, PE1, and VA1 IBX data center facilities are not staffed with dedicated onsite security guards. Each of the aforementioned sites are monitored by Equinix personnel remotely via other sites. Equinix has evaluated the need for onsite security staff at each of the locations and accepted the business risks based on the small footprint, low traffic volume, and limited customer bases at each site.

Other security features and controls may include:

- Control points between exterior and customer equipment.
- 90-day video activity storage (subject to local country law).
- 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 IBX functions in order to assure no local agreements.
- Customer privacy policies, including no pictures and customer anonymity.
- IBX data center facility design, which includes controlled access points, reinforced exterior walls.

- Token authentication required for access to enterprise network.
- Bullet-resistant protection (applicable to AMER only).
- Motion-detection lighting, and automatic lighting that is activated in the event of a power outage or disruption including IBX data center facility emergency exits.

Ingress mantraps are in place and administered to help restrict access to IBX facilities to only authorized individuals, else, there needs to be continuous monitoring of IBX access doors leading to the exterior. 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 IBX data center 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 colocation side of doors to exit the colocation area into the customer care / common areas. Entry to customer cages from the exterior to the IBX requires access from a minimum of three to four access controls.

Cage security is provided through multiple levels of access control: hand geometry readers at the cage entrance (subject to customer requirement), keyed locks at each cage or access card reader at each cage, and if the cabinet is located in a shared-cage environment, the cabinet door includes a lock. 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 the convenience of Equinix personnel.

The LA2 IBX data center 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 IBX data center 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 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.

The SL1, SH2, SH3, TY6, TY7, TY8, and TY9 IBX facilities were not constructed by Equinix. Size constraints limited the amount of remodeling that could be accomplished, and exceptions were allowed in the redesign. The TY6, TY7, TY8, and TY9 facilities attained from the Bit-Isle acquisition in 2015 and TY11 are not equipped with mantraps. Instead, TY8, TY9 and TY11 facilities are equipped with speed gates (security gate) in place to prevent unauthorized passage or tailgating. Additionally, HK3 1st floor (1-DC-2) has both biometric and mantrap capabilities, and 1-DC-1 is secured via card reader and fingerprint. HK3 6th floor (6-DC-1 and 6-DC-2) is secured via card reader and fingerprint, and TY1 (4th floor) is secured via biometric access card readers; both do not require mantrap entry to the colocation areas.

Access to each of the aforementioned facilities is monitored by 24x7 security guards and/or Equinix personnel, as well as through the use of security cameras located throughout the IBX data center facility. Mantraps are also in place at the entrances to the SH2 and SH3 facilities, and access to the colocation areas is controlled by use of two-factor authentication (2FA) security process monitored by the security and visitor registration office located at the entrance.

Employee IBX 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 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 and are given a proximity access card with specific access permissions assigned based on their role using a defined employee physical access matrix. It is Equinix company policy to issue identification badges to each Equinix employee and to temporary agency and contractor/contingent personnel. This policy applies to employees, trainees, temporary agency workers and Equinix

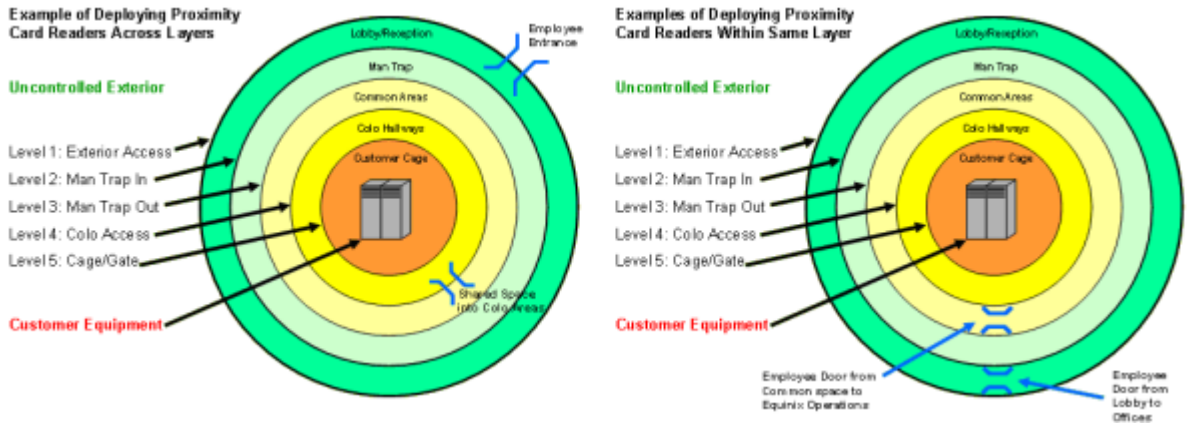
contractor personnel. Access is revoked once an employee is terminated or leaves the organization. Changes to employee roles and transfers also trigger an update to the access permissions assigned to an employee.

Personnel authorized to work at an Equinix IBX data center facility are required to display identification 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 IBX data center facility or monitored by CCTV cameras. Off-site employees are screened upon entry to verify their identity. The security guard checks the government issued photo identification and visitors are required to sign in. 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.

The Siebel ticketing system is a web-based portal that security personnel use to view and manage access requests.

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 along with intercom radio with camera are installed at vehicle access gates at some IBX locations, which control access to areas surrounding shipping/receiving doors and/or loading docks.

Proximity cards and keys are maintained at the security desk and are issued as needed. Proximity cards and keys are not authorized to be removed off-site. Security personnel perform a daily review of proximity cards and keys maintained and issued; any cards or keys that are unaccounted for are disabled and the event is reported to relevant operation management members for analysis and further communication (as applicable).



Temporary use badges are issued by IBX site personnel only upon receipt of written or electronic authorization from Equinix management. A temporary use badge may be issued to an employee in 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 IBX data center facility. Issuance of sign-out badges is also documented within a security form. Equinix management is notified if any badge is not returned within 24 hours of issuance.

Customer IBX Data Center Access

Customers are required to sign a contract and a nondisclosure agreement with Equinix. Customers, customer contractors and customer visitors are screened upon entry to verify their identity. Customers submit their requests either through ECP or GSD. Authorized customers are provided a unique identifier and password and granted access via specific roles within the ECP. ECP is the primary database for Equinix's customer contacts.

The security guard checks the government issued photo identification and visitors are required to sign in as per the Equinix IBX Access Process.

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. Customer requests (for work visits, access enrollment, tours, and/or remove access enrollment) are reviewed to make sure that they are authorized by an approved customer with ordering privileges. Requests are automatically transferred to the security system. The security guards set up the access based on the work visits or tours activities noted within Siebel. Customers accessing the IBX data center facility are required to display government issued valid identification when entering an Equinix IBX data center facility.

Vendor and Contractor IBX Data Center Access

Vendors and contractors are screened upon entry to verify their identity. The security guard checks the government issued photo identification and visitors are required to sign in. For an Equinix contractor, access permissions will be assigned in the ECP, or a work visit ticket will be created by an employee which automatically assigns relevant access permissions to the contractor for the activity. For a customer contractor, customers are responsible for assigning access permission or creating a Work Visit in ECP. In cases where the contractor requires access to a customer cage which has a documented and agreed space restriction, a Customer Space Restrictions Policy and Procedure is adhered to.

Visitor IBX Data Center Access

Visitors are screened upon entry to verify their identity. The security guard checks the government issued photo identification and visitors are required to sign in. Visitors also are required to read and accept a non-disclosure agreement before being granted access to the site. Visitors without an approved access enrollment are escorted to locations by authorized personnel.

Physical Access Removal

Removal of physical access rights to IBXs is the responsibility of the assigned customer and Equinix vendor administrator(s) to manage through ECP. Customer and Equinix vendor administrators must ensure they complete removal of any customer and vendor contacts through ECP in line with Equinix process. For Equinix employees and Equinix contingent workers, an automated system notification is triggered when an employee is terminated by HR, resulting in the removal of the employee's physical access rights from ECP.

Once customer, Equinix vendor, employee or Equinix contingent worker access is removed in ECP, access to the IBX is automatically removed on the relevant physical access control systems. Access removal activities are recorded in ECP for tracking purposes. The terminated employee ID badge and proximity card(s) are surrendered to line managers 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 the security service provider provides its officers and Equinix specific training once they are assigned to Equinix.

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
- IBX security policies and procedures
- Security officer responsibilities, including assigning access, access enrollment and access removal 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 complete training and both the trainer and trainee sign a checklist acknowledging the completion of the training. In addition to the training, the trainee is continuously monitored by the senior security officer on-site until he/she is comfortable and confident carrying out all the assigned responsibilities.

Equinix, in conjunction with its security providers, has developed a scorecard program for monitoring the performance of the security officers. The scorecard targets key performance indicators (KPI) that are focus areas mutually agreed-upon for the security 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.

Upon change of every shift, security guards perform a shift handover exercise during which there is an inventory check conducted on proximity cards and keys. Also, any security events encountered during the shift are communicated to the guards taking the next shift. All shift handover notes are frequently reviewed by IBX management to ensure adherence to Equinix security protocols.

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 also require permits, and IBX facilities are thus re-inspected for building code compliance. Equinix has comprehensive property insurance coverage for IBX facilities by a premier 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. The 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.

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 global Health and Safety program which is periodically audited and updated 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.
- 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 and upon receipt of an alarm the incident may be escalated to the city fire department if required. 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.

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. 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 automatic transfer switch which is also connected to redundant standby diesel or gas turbine 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 measure 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.

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 start up and run until the main fuel tanks are activated.

Separately installed main fuel tanks provide a source of fuel to engine generators. The sites are equipped with sufficient fuel storage onsite to support continuous operation at design load. Fuel capacity is monitored at all times with 75% capacity as the minimum at any time. Once fuel has reached 75% of capacity, fuel replenishment is initiated to return to at least 90% capacity (allowing 10% for expansion of the fuel). Equinix has contracts with multiple fuel providers for the fuel supply.

HVAC

Each IBX facility is designed with an HVAC system 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.

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 colocation 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 59 degrees and 89.6 degrees Fahrenheit (or between 15 degrees and 32 degrees Celsius). 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 59 degrees Fahrenheit (15 degrees Celsius).

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 based on IBX facility design. The leak detection system is monitored by the BMS.

Maintenance of Critical Systems

The IBX Critical Facilities personnel conduct regular engineering site rounds, which are documented. The rounds made are staggered to help ensure maximum equipment coverage.

Prior to the rounds, the IBX Critical Facilities engineer prints out a report from the BMS indicating alarm conditions, colocation area temperature and humidity readings, chiller loads, equipment statuses, and electrical loads. During the 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 aims to provide customers at least 37 days advance notice of scheduled 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 aims to provide three (3) to 36 days advance notice to customers. When emergency maintenance work is necessary, Equinix will aim to notify impacted customers immediately, or as soon as practically possible.

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, electromagnetic current testing methods, and vibration analysis, etc. Outside contractors will be used for some PdM tasks, as determined by the IBX Critical Facilities personnel.

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, a user must first authenticate through a zero trust platform (Zscaler Zero Trust Exchange) and establish an encrypted connection via client connector (Zscaler Client Connector) installed on authorized Equinix endpoints. The zero trust platform is 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. Network users, remote or on-premises, are required to authenticate via the zero trust platform prior being granted access to Equinix's network domain. Global group policies (GPOs) are utilized to govern predefined user account and predefined minimum password requirements for all network domain user accounts and authentication controls are inherited from the primary domain controller's GPOs. The in-scope systems, including server operating systems, databases, the firewall management console, physical access control systems, building management systems, and the applications (GSD, Siebel, IBM Maximo, ECP) are configured to require users to authenticate via a unique user account and password. Predefined security groups are utilized to assign role-based access privileges and segregate access to aforementioned in-scope systems and administrative access privileges to these systems are restricted to user accounts accessible by authorized personnel. Access to the ECP portal requires users to authenticate via a unique user accounts and password and is configured to enforce minimum password requirements.

Logical Access Requests and Access Revocation

Procedures exist and are followed to establish new user access privileges to the corporate network domain. Corporate IT personnel are responsible for administering and provisioning user access privileges to the network and underlying operating systems 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.

Network Security and Systems Monitoring

The firewall management console is used to centrally manage the firewalls in place to protect the organization's network. Firewalls are configured to filter unauthorized inbound network traffic from the internet and deny network connections not explicitly authorized by a firewall rule. In addition to the use of firewalls, policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. Data processors and owners are required to establish and implement processes and measures for the use of encryption protocols to protect sensitive in transit using strong cryptography and security protocols (e.g., TLS, IPSEC, SSH, etc.). To help enforce such policies, employees are required to utilize an encrypted internet gateway for access to the corporate environment to help establish secure connections and the ECP web servers are configured to utilize TLS 1.2 and TLS 1.3 encryption for encrypted web communication sessions.

Equinix's IT security team has implemented a centralized security information and event management (SIEM) tool to monitor and log certain predefined security events / activity for the in-scope systems. Event details logged by the SIEM tool include, but are not limited to, the security event detection time, security event severity rating, and source system from which the SIEM detected the security event. An intrusion detection system (IDS) is also in place to monitor and analyze network traffic. The IDS logs events identified as threats and includes event details such as, but not limited to, threat generation time, threat type (e.g., spyware or vulnerability), the source address of the threat, and the destination address of the threat. Security activity, events, and / or threats logged through the SIEM tool and IDS were monitored via dashboards.

Next generation antivirus/anti-malware software is configured to scan and monitor registered workstations and production endpoints in real time for abnormal and malicious behavior using behavioral analytics. The software uses signatureless protection to expose threats in near real time with machine learning.

Media Handling

Asset removal and disposal policies are in place to guide personnel in the disposal of assets to ensure data and software are unrecoverable prior to retiring a physical asset. Asset owners are responsible for the overall management of the respective media or equipment, approval of the transportation method for the media, and approval of the media disposal request. Asset custodians are responsible for confirming the secure destruction of the data inside the media before disposal. A disposal service contractor is then used to complete the destruction and disposal of assets.

Change Management

A change control process is documented and implemented to provide a framework for documentation, testing, and approval of proposed changes to both infrastructure and applications. Information security is considered for all projects related to the changes of Equinix applications and Infrastructure. Changes are categorized by deployment urgency:

- *Standard* change implementations follow the normal schedule and are reviewed and approved during weekly change review board (CRB) meetings.
- *Urgent* change implementations require out-of-cycle approval (i.e. approval before the next CRB review meeting) to resolve an urgent issue or fulfill an urgent request.
- *Emergency* change implementations requiring immediate implementation are required to resolve a priority (P1) issue and cannot wait for CRB approval; generally, the change request is created as an after-the-fact for documentation purposes.

Ongoing and upcoming projects that require infrastructure and / or application changes are reviewed, discussed, prioritized and scheduled during weekly CRB meetings. A formal change request must be submitted via a ticketing system for infrastructure and application changes, which includes details such as, but not limited to, the change category, region affected, functional area, and classification. The ticketing system is further used to document, manage, and track change reviews, approvals, and as needed, user acceptance testing. Application changes are required to undergo testing, which could include unit, functional, integration, and / or user acceptance in test environments logically segmented from the production environment. Once the relevant testing has been completed and the necessary approvals are received, the change is scheduled for implementation. Access to promote changes into the production environment is restricted to user accounts accessible by authorized personnel.

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 systems are in place to perform scheduled and manual backups of IBX data and systems at predefined times. 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.

Business Continuity Management

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 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 schedule and conduct exercises on the BRP.

Plan Responsibility and Maintenance		
Maintenance / Test / Exercise	**Responsible**	**Minimum Frequency**
Maintain emergency contact list	IBX manager	Quarterly
Review threat and risk assessment and business recovery plan, and advise global operations enablement / support of required updates	IBX manager	Annual
Plan and conduct IT application and system exercises (enterprise servers)	Global IT	
Plan data retention	Business Continuity Program Office	Every 7 years
Maintenance of critical equipment including generators, UPS, fire detection, fire suppression, BMS, HVAC, and comprehensive utility failure test	Critical Engineering – for mechanical, electrical, and plumbing (MEP) infrastructure	Annual

Plan Responsibility and Maintenance		
Maintenance / Test / Exercise	**Responsible**	**Minimum Frequency**
Maintenance of access control system equipment, CCTV	IBX manager	Monthly, quarterly, semi-annual, annual
Business continuity drill		Annual
Evacuation drill		Semi-annual
Engineering drill		Quarterly
Environmental drill		Annual
Bridge communication drill		Annual
Equinix notice	Business Continuity Program Office	Semi-annual
Business recovery plan test –site team leads and above		Annual
Crisis management team exercise / response to actual event		

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)

Data center facility incidents and corrective measures are reported monthly for management review to ensure that the incident response procedures were followed, and that the incident was resolved. 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, action items, and where applicable, lessons learned.

Incident response plan testing exercises using simulated 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 is in place to promote incident response plan awareness. Data center operations personnel are required to participate in the training program at least annually 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 security incidents. CMT personnel are also educated on the latest cyber threats and vulnerabilities that could potentially impact the company during the annual meeting.

Data

Customers are responsible for the data maintained within their environments. Within the scope of the Global Data Center Housing 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 housing services, includes, but is not limited to, the following:

- Biometrics, proximity card, and PIN code access history logs, including access history and security alarms.
- 90-day video activity storage (subject to local country law).
- Alert notifications and monitoring reports generated from the environmental monitoring applications and the BMS.
- Enterprise monitoring applications are utilized to monitor the performance and availability of production servers and network infrastructure.
- Security monitoring applications are utilized to monitor and log certain security events for the in-scope systems and analyze network traffic for possible or actual security breach events.
- Incident / issue reports documented via the ticketing systems.

Significant Changes During the Period

During the period, Equinix opened the DB6x, WA4x, MD3x, and ML7x data centers. The suitability of the design and operating effectiveness of controls to achieve the related control objective stated in the description of the Global Data Center Housing Services system were examined at the new IBX data center facilities in accordance with the site go-live dates, as follows:

- Dublin 6 (DB6x) IBX data center facility for the period May 1, 2024, to October 31, 2024
- Warsaw 4 (WA4x) IBX data center facility for the period May 1, 2024, to October 31, 2024
- Madrid 3 (MD3x) IBX data center facility for the period May 1, 2024, to October 31, 2024
- Milan 7 (ML7x) IBX data center facility for the period December 1, 2023, to October 31, 2024

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

Subservice Organizations

The facility environmental protection control services provided by Digital Realty at the CH4 IBX data center, Samsung SDS at the SL1 data center, BT Communications Ireland at the DB1 IBX data center, and Khazna at the DX2 and AD1 IBX data centers were not included within the scope of this examination.

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

Control Activity Expected to be Implemented by Digital Realty, Samsung SDS, BT Communications Ireland, and Khazna	Applicable Trust Services Criteria
Digital Realty, Samsung SDS,BT Communications Ireland, and Khazna are responsible for ensuring that the facility environmental security controls for the colocation space, backup media storage, and other sensitive locations (including maintenance of sensitive system components within these locations) at the Chicago 4 (CH4), Seoul 1 (SL1),Dublin 1 (DB1), Dubai 2 (DX2) and Abu Dhabi (AD1) data center facilities are designed, monitored, and operating effectively.	A1.2, A1.3

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 board of directors and senior leadership 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:

- Equinix's code of conduct is included within the employee handbook to communicate company values and behavioral standards to personnel.
- 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.
- New hires are required to sign an employee agreement consenting to not disclose confidential or proprietary client and company information to unauthorized parties.
- Background and reference checks are conducted for new hire employees, subject to local laws.

Board of Directors and 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.

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 to help 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. Members of top management meet 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. Specific control activities that Equinix has implemented in this area are described below:

- Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel. Updates to the organizational charts are communicated to employees via e-mail.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- The board of directors and senior management team has assigned authorities for defining and implementing security policies to the chief information security officer.
- Members of top management meet, 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.

Commitment to Competence

Equinix management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. A third-party web application is utilized during the hiring process to qualify the skills of applicants within certain job functions. 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. As a result, position requirements are translated into written required skills and knowledge levels. 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. Specific control activities that Equinix has implemented in this area are described below:

- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Training courses are available to new and existing employees to maintain and advance the skill level of personnel.

- Employees are required to complete new hire security awareness training and security awareness training on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Management conducts a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.

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:

- 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.
- Management conducts a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.
- 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.
- 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.
- New hires are required to complete an acknowledgment form upon hire the handbook and company policies consenting to not disclose confidential or proprietary client and company information to unauthorized parties.
- Management provides internal control performance metrics to the information security management committee (ISMC) on an annual basis and documents the metrics in internal control performance dashboards for ISMC review.

RISK ASSESSMENT

Equinix's management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. Equinix's 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 the 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.
- After an information security incident.

Objective Setting

Equinix considers the needs and expectations of interested parties and the boundaries of its Global Data Center Housing 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, which is an essential part of the process, and understanding the potential threats and vulnerabilities that could threaten its ability to achieve said objectives. Senior leadership and operations management has committed to customers to carry out certain objectives in relation to the Global Data Center Housing Services provided. These objectives (commitments) are documented and formally reviewed by management 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 and Analysis

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 or equal to 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 IBX data centers that has value and requires protection. The risk assessment procedure, and threat and risk assessment surveys for each data

center IBX data center 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, economical, and political threats. The operations manager completing the survey may include additional risks within each hazard type specific to their site, as needed.

Risk Factors

Management 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
- A disruption in information systems processing that could adversely affect the entity's operations
- The quality of personnel hired and methods of training and motivation that could influence the level of control consciousness within the entity
- A change in management responsibilities that could affect the way certain controls are affected
- The nature of the entity's activities, and employee accessibility to assets, that could contribute to misappropriation of resources
- Types of fraud, fraud opportunities, fraud incentives and pressures for employees, and employee attitudes and rationalizations for fraud

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 (P)
- Risks:
    - Human Impact (HI)
    - Properly Impact (PI)
    - Business Impact (BI)
- Mitigation measures:
    - Planning and preparedness (PP)
    - Internal Resources (IR)
    - External Resources (ER)

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			
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; IBX data center 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		
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 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 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 realizes 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 the documented risk assessment policies and procedures guide personnel in identifying and analyzing risks including the potential for fraud.

Risk Mitigation

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.

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. 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. A key controls matrix is documented and maintained to identify control activities used to support the achievement of objectives along with control justifications and a description of how the control activities are implemented. Documented policies and procedures are also 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. 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.

Additionally, employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.

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

INFORMATION AND COMMUNICATION SYSTEMS

Relevant Information

Information is necessary for Equinix to carry out internal control responsibilities to support the achievement of its objectives related to the Global Data Center Housing Services system. Equinix's internal systems supporting the Global Data Center Housing Services include 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 IBX 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 IBX data centers are interconnected by a dedicated data link with internet service providers to facilitate internet access.

Management obtains or generates and uses relevant internal and external information sources to support the functioning of internal control. Security policies and procedures are documented that identify the information required to support the functioning of internal control and the achievement of objectives. Internal data resources used by Equinix include alert notifications and reports generated from security monitoring systems as well as infrastructure and BMS monitoring applications used for monitoring system availability and capacity levels. The organization also conducts internal audits to provide independent and objective reviews and assessments of business activities, operations, and internal controls at IBX facilities. A risk-based sampling approach is applied for selection of internal audits performed at IBX facilities on an annual basis. Control and process deficiencies identified as a result of the internal audits are documented and tracked through resolution by security and compliance personnel. Results of the internal audits including corrective action plans for control deficiencies are reported to and reviewed with management.

External data sources used by Equinix to support the functioning of internal control include monthly network vulnerability assessments, annual penetration testing of the customer web portal, and corresponding vulnerability remediation plans; third-party preventative maintenance to test and confirm the operations of IBX environmental systems; and third-party reported security KPIs for facilities that employ onsite security guards. Equinix's global information security group also subscribes to subscription based security notifications to monitor the security impact of emerging technologies and threats.

Communication

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.

Other examples of internal communication methods are included below:

- 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.
- 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.
- 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.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for specific jobs.
- Documented policies and procedures for reporting incidents are in place to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.
- A CRB is held on a weekly basis to discuss and communicate the ongoing and upcoming change projects that affect the system.

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 direct relations with Equinix personnel. If incidents are communicated through the online portal, personnel follow documented incident response plan. Incidents are processed according to Equinix global procedures following the Equinix global incident flowchart. Incidents are documented within the ticketing system and tracked by management until resolved. Other examples of external communication methods are included below:

- Equinix's security and availability commitments and the associated system requirements are documented and communicated via IBX policies published on the company website.
- Customers are required to sign a contract stating Equinix's security and availability commitments, the associated system requirements, and a nondisclosure agreement.
- Changes, incidents, and outages related to security and availability at the data centers are communicated to customers and external users of the system via e-mail advisory notifications. If incidents are communicated through the online portal, personnel follow documented incident response plan. Incidents are processed according to Equinix global procedures following the Equinix global incident flowchart and are documented within the ticketing system and tracked by management until resolved.
- Customer end-users are provided with access to the ECP and procedures for contacting the GSD to report incidents, concerns, or complaints related to security and availability.

MONITORING

Monitoring Activities

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, but not limited to:

- System and Organization Controls (SOC) 1 / ISAE 3402 and SOC 2 / ISAE 3000 Examinations
- International Organization for Standardization (ISO) 27001, ISO 22301 and ISO 9001
- Environmental, Energy, Health and Safety Standards: ISO 45001, ISO 50001 and ISO 14001
- Payment Card Industry Data Security Standards (PCI DSS)
- National Institute of Standards and Technology (NIST) 800-53 – U.S. only
- Health Insurance Portability and Accountability Act (HIPAA) – U.S. only
- Tier III Design, Facility and Operations
- Sarbanes-Oxley (SOX)
- Cyber Essentials – EMEA only
- Health Data Hosting (HDS) – EMEA only

Monitoring of Subservice Organizations

Equinix's CH4 IBX data center facility is located in the same multi-tenant building as the CH1 and CH2 IBX data center facilities. Facility engineers and security personnel located on-premises at the adjacent CH1 and CH2 IBX data centers are tasked with directly monitoring the CH4 facility and the environmental protection system controls provided by Digital Realty. 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 South Korea metropolitan area are tasked with directly monitoring the SL1 facility and the environmental protection system controls provided by Samsung SDS. Services provided by Samsung SDS are monitored through phone and e-mail communications, meetings, and the service provider's customer web portals.

Equinix operations personnel local to the Dublin metropolitan area are tasked with monitoring the DB1 facility and the environmental protection system controls provided by BT Communications Ireland. Services provided by BT Communications Ireland are monitored via phone, e-mail, and / or scheduled meetings, as needed, and notifications from the service provider to local Equinix operations personnel.

Similarly, Equinix operations personnel local to the Dubai and Abu Dhabi metropolitan areas are responsible for monitoring the DX2 and AD1 facility and environmental protection controls provided by Khazna. Services provided by Khazna are monitored via phone, e-mail, and / or scheduled meetings, as needed, and notifications from the service provider to local Equinix operations personnel.

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

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

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Global Data Center Housing Services system provided by Equinix. The scope of the testing was restricted to the Global Data Center Housing Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period November 1, 2023, through October 31, 2024.

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 handbook to communicate company values and behavioral standards to personnel.	Inspected the global Equinix Code of Business Conduct and employee handbooks for a sample of countries where the in-scope IBX data centers reside to determine that Equinix's code of conduct was included within the employee handbooks to communicate the company's values and behavioral standards to personnel for each country sampled.	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 policy acknowledgments for a sample of employees hired during the period to determine that each employee sampled completed an acknowledgement form indicating they had been given access to 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 policy acknowledgments for a sample of employees hired during the period to determine that each employee sampled completed an acknowledgement form consenting to not disclose confidential or proprietary, client and company information to unauthorized parties.	No exceptions noted.
CC1.1.4	Background and reference checks are conducted for new hire employees, subject to local laws.	Inspected the background and reference check results for a sample of employees hired during the period to determine that a background and/or reference check was completed, subject to local laws, 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 implementing security policies to the chief information security officer.	No exceptions noted.
CC1.2.2	Members of top management meet, 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 management review procedure, and the most recent annual management meeting minutes to determine that members of top management met globally and regionally during the 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. Updates to the organizational charts are communicated to employees via e-mail.	Inspected the global company organizational charts and an example update notification sent during the 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 IBX facilities, operations, support, and management 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 implementing security policies, related to the achievement of its objectives to the chief information security officer.	No exceptions noted.
CC1.3.4	Members of top management meet, 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 management review procedure, and the most recent annual management meeting minutes to determine that members of top management met globally and regionally during the 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 global operations compliance senior 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the corporate training portal and example training course documentation made available 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.
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 period to determine that 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 employees to determine that security awareness training was completed during the period for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
CC1.4.4	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 resource business partner regarding the employee performance evaluation procedures to determine management conducted a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.	No exceptions noted.
		Inspected the most recent 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 period for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.5	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for IBX facilities, operations, support, and management 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.
CC1.5 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 and 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 maintained on the company's ethics and compliance hub 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.	Inquired of the human resource business partner regarding the employee performance evaluation procedures to determine management conducted a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.	No exceptions noted.
		Inspected the most recent performance review documentation for a sample of current employees to determine that an evaluation of individual performance against expected levels of performance and conduct was performed during the period for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.4	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 period to determine that 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 employees to determine that security awareness training was completed during the period for each employee sampled to understand their obligations and responsibilities to comply with company security policies.	No exceptions noted.
CC1.5.5	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 policy acknowledgments for a sample of employees hired during the period to determine that each employee sampled completed an acknowledgement form indicating they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within.	No exceptions noted.
CC1.5.6	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 policy acknowledgments for a sample of employees hired during the period to determine that each employee sampled completed an acknowledgement form consenting to not disclose confidential or proprietary, client and company information to unauthorized parties.	No exceptions noted.
CC1.5.7	Management provides internal control performance metrics to the ISMC on an annual basis and documents the metrics in internal control performance dashboards for ISMC review.	Inspected the most recent annual management global and regional meeting minutes and performance metrics dashboard to determine that internal control performance metrics were documented within internal control performance dashboards for review with the ISMC during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	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.
CC2.1.2	Internal data sources are used to obtain relevant and quality information to support the functioning of internal control, including the following: · Security and enterprise monitoring system alert notifications · Infrastructure and BMS monitoring applications to monitor system availability and capacity levels · Annual internal audit and tracking of identified issues through resolution	Inspected the following security assessments and monitoring activities performed during the period to determine that internal data sources were used for the purposes of obtaining relevant and quality information to support the functioning of internal control during the period, that included the following: · Security and enterprise monitoring system alert notifications · Infrastructure and BMS monitoring application dashboards and example alert notifications to monitor system availability and capacity levels · Annual internal audit and tracking of identified issues through resolution	No exceptions noted.
CC2.1.3	External data sources are used to obtain relevant and quality information to support the functioning of internal control, including the following: · Monthly network vulnerability assessments and related remediation plans · Annual penetration testing for the customer web portal and related remediation plans · Preventative maintenance reports to test and confirm the operations of environmental systems · Security KPIs for facilities that employ onsite security guards	Inspected the following security assessments and monitoring activities performed during the period to determine that external data sources were used to support the functioning of internal control during the period, that included the following: · Monthly network vulnerability assessments and related remediation plans · Annual penetration testing for the customer web portal and related remediation plans · Preventative maintenance reports to test and confirm the operations of environmental systems · Security KPIs for facilities that employ onsite security guards	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 period to determine that the entity's global information security group monitored the security impact of emerging technologies and threats and notified relevant personnel.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	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 policies and procedures maintained on the company 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 period to determine that 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 employees to determine that security awareness training was completed during the 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 IBX facilities, operations, support, and management 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 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.
CC2.2.5	A CRB meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming change projects that affect the system.	Inspected the CRB meeting documentation for a sample of weeks during the period to determine that a CRB meeting was held to discuss and communicate the ongoing and upcoming change 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	Customers are required to sign contracts stating Equinix's security and availability commitments, the associated system requirements, and a nondisclosure agreement.	Inspected the global terms and conditions contracts and nondisclosure agreements for a sample of customers onboarded during the period to determine that signed contracts and a nondisclosure agreement stating Equinix's security and availability commitments, associated system requirements were in place for each customer sampled.	No exceptions noted.
CC2.3.2	Equinix's security and availability commitments and the associated system requirements were documented and communicated via IBX policies published to the company website.	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.
CC2.3.3	Changes, incidents, and outages related to security and availability at the data centers are communicated to customers and external users of the system via e-mail advisory notifications.	Inspected the external advisory notification for a sample of incidents closed during the period to determine that changes, incidents, and outages related to security and availability at the data centers were communicated to customers and external users of the system via e-mail advisory notifications for each incident sampled.	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 to security and availability.	Inspected the IBX policies and procedures and GSD contact information published on 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.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	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 standard risk assessment 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 threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled 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 mitigation 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, procedures, and standard risk assessment 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.

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 threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled 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 housing services are maintained for review during the annual risk assessment process.	Inquired of the operations compliance senior specialist regarding the risk assessment procedures to determine that asset inventory listings of hardware and systems required for the provision of data center housing 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 centers to determine that asset inventory listings of equipment required for the provision of the data center housing services was maintained for each IBX data center 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 information security risk management policies and procedures are in place to guide personnel in identifying and analyzing risks including the potential for fraud.	Inspected the risk assessment policies, procedures, and standard risk assessment templates to determine that documented information security risk management policies and procedures were in place to guide personnel in identifying and analyzing risks including the potential for fraud.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3.2	A risk assessment is performed on an annual basis that considers the risks related to the achievement of objectives, including the potential for fraud. 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 threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled that considered the identification and assessment of risks relating to the achievement of objectives, including the potential for fraud, and that risks were identified using a risk evaluation process and formally documented, along with activities, for management review.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	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, procedures, and standard risk assessment templates 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 considers the identification and assessment of risks that could significantly impact the system of internal control. 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 threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled that considered the identification and assessment of risks that could significantly impact the system of internal control, 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 period to determine that the entity's global information security group monitored the security impact of emerging technologies and threats and notified relevant personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Security assessments and monitoring activities are performed to help ensure that components of internal control are present and functioning, and include, but are not limited to, the following: · Monthly network vulnerability assessments and related remediation plans · Annual penetration testing for the customer web portal and related remediation plans · Preventative maintenance reports to test and confirm the operations of environmental systems · Security KPIs for facilities that employ onsite security guards · Annual internal audit and tracking of identified issues through resolution	Inspected the following security assessments and monitoring activities performed during the period to determine that security assessments and monitoring activities were performed to help ensure that components of internal control were present and functioning during the period, that include the following: · Monthly network vulnerability assessments and related remediation plans · Annual penetration testing for the customer web portal and related remediation plans · Preventative maintenance reports to test and confirm the operations of environmental systems · Security KPIs for facilities that employ onsite security guards · Annual internal audit results including the corrective action tracking plan completed	No exceptions noted.
CC4.1.2	Information security audit and compliance assessments are conducted by accredited independent third-party assessors on an annual basis. The results of the assessments are reviewed by management.	Inspected the most recently completed third-party information security audit and compliance assessments and the management review meeting presentation to determine that information security audit and compliance assessments were conducted by accredited independent third-party assessor and results of the assessments were reviewed by management 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	Risk treatment activities are documented, tracked, and communicated to those parties responsible for taking corrective action on internal control deficiencies.	Inspected the most recent annual threat and risk assessments and mitigation tracking documentation for a sample of IBX data centers to determine that risk treatment activities were documented, tracked, and communicated to parties' responsible parties for taking corrective action during the review period for each IBX data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Members of top management meet, 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 management review procedure, and the most recent annual management meeting minutes to determine that members of top management met globally and regionally during the period to review security, compliance and operational metrics related to the achievement of the company's information security objectives.	No exceptions noted.
CC4.2.3	Information security audit and compliance assessments are conducted by accredited independent third-party assessors on an annual basis. The results of the assessments are reviewed by management.	Inspected the most recently completed third-party information security audit and compliance assessments and the management review meeting presentation to determine that information security audit and compliance assessments were conducted by accredited independent third-party assessor and results of the assessments were reviewed by management during the period.	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 annual threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled that considered the identification and assessment of risks relating to objectives and that mitigation strategies included the selection and development of general 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 annual threat and risk assessments and mitigation tracking documentation for a sample of IBX data centers to determine that risk treatment activities were documented, tracked, and communicated to parties' responsible parties for taking corrective action during the review period for each IBX data center sampled.	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 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 statement of applicability 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	Risk treatment activities are documented, tracked, and communicated to those parties responsible for taking corrective action on internal control deficiencies.	Inspected the most recent annual threat and risk assessments and mitigation tracking documentation for a sample of IBX data centers to determine that risk treatment activities were documented, tracked, and communicated to parties' responsible parties for taking corrective action during the review period for each IBX data center sampled.	No exceptions noted.
CC5.2.2	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 annual threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled that considered the identification and assessment of risks relating to objectives and that mitigation strategies included the selection and development of general control activities by assigned risk owners were documented for management review.	No exceptions noted.
CC5.2.3	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 statement of applicability 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	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.
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 and including termination, for violation to company policies and the code of conduct.	No exceptions noted.
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 period to determine that 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 employees to determine that security awareness training was completed during the 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.	Inspected the network domain authentication configurations to determine that the corporate network domains were configured to require users to authenticate via a user account and enforce minimum password requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the authentication configurations for a sample of production server operating systems and databases to determine that the operating systems and databases were configured to require users to authenticate via a user account and password for each system sampled.	No exceptions noted.
		Inspected the firewall management console authentication configurations to determine that the centralized firewall management system was configured to require users to authenticate with their network user account and password credentials via single-sign on.	No exceptions noted.
		Inspected the physical access control system authentication configurations for a sample of IBX data centers to determine that the physical access control systems were configured to require users to authenticate via a user account and password for each IBX data center sampled.	No exceptions noted.
		Inspected the BMS authentication configurations for a sample of IBX data centers to determine that the BMS were configured to require users to authenticate via a user account and password for each IBX data center sampled.	No exceptions noted.
		Inspected the authentication configurations for the in-scope applications (GSD, Siebel, IBM Maximo, ECP) to determine that the applications were configured to require users to authenticate with their network user account and password credentials via single-sign on.	No exceptions noted.
CC6.1.2	A zero trust network access solution is utilized to establish secure connections and is configured to enforce two-factor authentication requirements for access to the corporate network.	Inspected the zero trust network access solution user authentication and encryption policy configurations to determine that a zero trust network access solution was utilized to establish secure connections and was configured to enforce two-factor authentication requirements to the corporate network.	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 for the in-scope systems.	Inspected the network domain user account and role assignments listings with the assistance of the senior infrastructure engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the corporate network domain.	No exceptions noted.
		Inspected the user account and role assignment listings for a sample of production server operating systems and databases with the assistance of the operations compliance manager and senior information security engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for each system sampled.	No exceptions noted.
		Inspected the firewall management console user account and role assignment listings console with the assistance of the senior information security engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the centralized firewall management system.	No exceptions noted.
		Inspected the physical access control system user account and role assignment listings for a sample of IBX data centers with the assistance of the operations compliance manager to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the physical access control systems for each IBX data center sampled.	No exceptions noted.
		Inspected the user account and role assignments listings for the in-scope applications (GSD, Siebel, IBM Maximo, ECP) with the assistance of senior information security engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the applications.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the network domain administrator user account listing with the assistance of the senior infrastructure engineer to determine that administrative access privileges to the corporate network domain were restricted to authorized personnel.	No exceptions noted.
		Inspected the administrator user account listings for a sample of production server operating systems and databases with the assistance of the senior information security engineer to determine that administrative access privileges to the operating systems and databases were restricted to authorized personnel for each system sampled.	No exceptions noted.
		Inspected the firewall management console administrator user account listing with the assistance of the senior information security engineer to determine that administrative access privileges to the centralized firewall management system were restricted to authorized personnel.	No exceptions noted.
		Inspected the physical access control system administrator user account listings for a sample of IBX data centers with the assistance of the operations compliance manager to determine that administrative access privileges to the physical access control systems were restricted to authorized personnel for each IBX data center sampled.	No exceptions noted.
		Inspected the BMS administrator user account listings for a sample of IBX data centers with the assistance of the operations compliance manager to determine that administrative access privileges to the BMS were restricted to authorized personnel for each IBX data center sampled.	No exceptions noted.
		Inspected the administrator user account for the in-scope applications (GSD, Siebel, IBX Maximo, ECP) with the assistance of senior information security engineer to determine that administrative access privileges to the applications were restricted to authorized personnel for each IBX data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Procedures exist and are followed to establish new user access privileges to the corporate network domain.	Inspected the user access request tracking documentation for a sample of employees hired during the period to determine that procedures existed and were followed to establish new user access privileges to corporate network domain for each employee sampled.	No exceptions noted.
CC6.2.2	Procedures exist and are followed to revoke corporate network domain access upon termination of employment.	Inspected the termination notification e-mail and evidence of corporate network domain user access revocation for a sample of employees terminated during the period to determine that procedures existed and were followed to revoke corporate network domain access upon termination of employment 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 the corporate network domain.	Inspected the user access request tracking documentation for a sample of employees hired during the period to determine that procedures existed and were followed to establish new user access privileges to corporate network domain for each employee sampled.	No exceptions noted.
CC6.3.2	Procedures exist and are followed to revoke corporate network domain access upon termination of employment.	Inspected the termination notification e-mail and evidence of corporate network domain user access revocation for a sample of employees terminated during the period to determine that procedures existed and were followed to revoke corporate network domain access upon termination of employment 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 for the in-scope systems.	Inspected the network domain user account and role assignments listings with the assistance of the senior infrastructure engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the corporate network domain.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user account and role assignment listings for a sample of production server operating systems and databases with the assistance of the operations compliance manager and senior information security engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for each system sampled.	No exceptions noted.
		Inspected the firewall management console user account and role assignment listings console with the assistance of the senior information security engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the centralized firewall management system.	No exceptions noted.
		Inspected the physical access control system user account and role assignment listings for a sample of IBX data centers with the assistance of the operations compliance manager to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data to the physical access control systems for each IBX data center sampled.	No exceptions noted.
		Inspected the user account and role assignments listings for the in-scope applications (GSD, Siebel, IBM Maximo, ECP) with the assistance of senior information security engineer to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the applications.	No exceptions noted.
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the network domain administrator user account listing with the assistance of the senior infrastructure engineer to determine that administrative access privileges to the corporate network domain were restricted to authorized personnel.	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 production server operating systems and databases with the assistance of the senior information security engineer to determine that administrative access privileges to the operating systems and databases were restricted to authorized personnel for each system sampled.	No exceptions noted.
		Inspected the firewall management console administrator user account listing with the assistance of the senior information security engineer to determine that administrative access privileges to the centralized firewall management system were restricted to authorized personnel.	No exceptions noted.
		Inspected the physical access control system administrator user account listings for a sample of IBX data centers with the assistance of the operations compliance manager to determine that administrative access privileges to the physical access control systems were restricted to authorized personnel for each IBX data center sampled.	No exceptions noted.
		Inspected the BMS administrator user account listings for a sample of IBX data centers with the assistance of the operations compliance manager to determine that administrative access privileges to the BMS were restricted to authorized personnel for each IBX data center sampled.	No exceptions noted.
		Inspected the administrator user account for the in-scope applications (GSD, Siebel, IBX Maximo, ECP) with the assistance of senior information security engineer to determine that administrative access privileges to the applications were restricted to authorized personnel for each IBX data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Procedures exist and are followed to establish and make changes to physical access privileges for customers.	Inquired of the data center site managers and security personnel regarding the physical access procedures to IBX data centers to determine that procedures were in place and followed to establish and make changes to physical access privileges for customers.	No exceptions noted.
		Inspected the site access request tracking documentation for a sample of customers onboarded during the period to determine that procedures were in place and followed to establish physical access privileges for each customer sampled.	No exceptions noted.
		Inspected the site access removal request tracking documentation for a sample of customers terminated during the period to determine that procedures were in place and followed to remove physical access privileges for each customer sampled.	No exceptions noted.
CC6.4.2	Procedures exist and are followed to establish and make changes to IBX physical access privileges for Equinix employees who have a need to access an IBX.	Inquired of the data center site managers and security personnel regarding the physical access procedures to IBX data centers to determine that procedures were in place and followed to establish and make changes to physical access privileges for Equinix employees who had a need to access an IBX data center.	No exceptions noted.
		Inspected the access request tracking documentation for a sample of IBX data center employees hired during the period to determine that procedures were in place and followed to establish IBX data center physical access privileges for each employee sampled.	No exceptions noted.
		Inspected the access removal request tracking documentation and evidence of access card removal from the IBX physical access control systems for a sample of IBX data center employees terminated during the period to determine that procedures were in place and followed to remove IBX data center 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
CC6.4.3	For offsite employees, customers, vendors, and contractors, onsite security or Equinix personnel review valid government issued photo identification prior to allowing access to IBX data centers.	Inquired of the data center site managers and security personnel regarding the physical access procedures to IBX data centers to determine that for offsite employees, customers, vendors, and contractors, onsite security or Equinix personnel were required to review valid government issued photo identification prior to allowing access to IBX data centers.	No exceptions noted.
		Observed the physical access procedures at the IBX data centers with the assistance of the data center site managers and security personnel to determine that onsite security or Equinix personnel reviewed valid government issued photo identification prior to allowing visitors access to each IBX data center.	No exceptions noted.
CC6.4.4	Visitor access procedures are in place requiring: · Visitor sign into a log upon entry to the IBX data center facilities · Visitors are to be escorted by an authorized employee when accessing the IBX data center facilities	Inquired of the data center site managers and security personnel regarding the visitor physical access procedures to the IBX data centers to determine that visitor access procedures were in place and required visitors to sign into a log upon entry to the IBX data center facilities and be escorted by an authorized employee when accessing the IBX data center facilities.	No exceptions noted.
		Observed the visitor access procedures at the IBX data centers with the assistance of the data center site managers and security personnel to determine that visitors were required to sign into a log upon entry to each IBX data center facility and be escorted by an authorized employee when accessing each IBX data center.	No exceptions noted.
		Inspected the visitor access log for a sample of IBX data centers and months during the period to determine that visitors signed into a log upon entry to the facility for each IBX data center and month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.5	Dual control biometric, four-digit personal identification numbers, and / or proxy card readers are in place to help ensure that only authorized individuals have the ability to access the IBX data center, warehouse area, and storage cages. This control shall be applied as and where applicable.	Observed the site entrances and doors throughout the IBX data centers with the assistance of the data center site managers and security personnel to determine that a dual control biometric, minimum four-digit PIN, and / or proxy card readers were in place to help ensure that only authorized individuals had the ability to access each IBX data center, warehouse area, and storage cages, and that the control was applied as and where applicable.	No exceptions noted.
		Inspected the physical access control user assignment listings for a sample of IBX data centers to determine that dual control biometric readers, four-digit personal identification numbers, and / or proxy card readers were in place for each IBX data center sampled.	No exceptions noted.
CC6.4.6	Biometric hand scan and / or proxy card access to the IBX data centers is electronically logged and maintained as per data privacy laws. Exceptions or attempts of unauthorized access are tracked and escalated.	Inquired of the data center site managers and security personnel regarding the physical access logging and exception escalation procedures to determine that biometric hand scan and / or proxy card access to the IBX data centers was electronically logged and maintained, as per data privacy laws, and that exceptions or attempts of unauthorized access were tracked and escalated.	No exceptions noted.
		Observed the historical physical access system logs and the access exception procedures for the IBX data centers with the assistance of the data center site managers and security personnel to determine that biometric hand scan and / or proxy card access was electronically logged and maintained as per data privacy laws, and that procedures were in place to track and escalate exceptions attempts of unauthorized access for each IBX data center.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the historical access control system logs retained for a sample of IBX data centers to determine that biometric hand scan and / or proxy card access was electronically logged, including attempts of unauthorized access, and maintained for at least 12 months or as per local data privacy laws for each IBX data center sampled.	No exceptions noted.
CC6.4.7	Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.	Observed the surveillance camera systems and security monitoring procedures throughout the IBX data centers with the assistance of the data center site managers and security personnel to determine that internal and external monitoring of data center activity was performed through the use of security guard personnel and / or surveillance cameras at each IBX data center.	No exceptions noted.
		Inspected the security guard shift schedule for a sample of IBX data centers and months during the period to determine that security guard personnel were scheduled 24x7 to monitor data center activity for each IBX data center and month sampled.	No exceptions noted.
CC6.4.8	CCTV surveillance cameras are in place to monitor and record activity at the entrances to and throughout the IBX data center facilities. Surveillance camera logs are recorded and maintained minimum of 90 days unless specified otherwise per local country law/regulation for IBX data center facilities.	Observed the CCTV surveillance cameras throughout the IBX data centers with the assistance of the data center site managers and security personnel to determine that CCTV surveillance cameras were in place to monitor and record activity at the entrances to and throughout each IBX data center.	No exceptions noted.
		Inspected the historical surveillance camera logs maintained for a sample of IBX data centers to determine that surveillance camera logs were recorded and maintained for a minimum of 90 days unless otherwise per local country law/regulation for each IBX data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.9	Ingress mantraps are in place and administered to restrict access to IBX data center facilities to only authorized individuals. Else, there needs to be continuous monitoring of IBX access doors leading to the exterior.	Observed the site entrances and doors throughout the IBX data centers with the assistance of the data center site managers and security personnel to determine that ingress mantraps were in place and administered to restrict access to each IBX data center facility; for IBX data center facilities where a mantrap was not in place, observed the security desk which continuously monitored the doors leading to the exterior of each IBX data center.	No exceptions noted.
CC6.4.10	Each customer has a defined space within the IBX data center that is physically secured within a locked cage and / or cabinet.	Observed the locked cages and / or cabinets at the IBX data centers with the assistance of the data center site managers and security personnel to determine that customers had defined space that was physically secured within a locked cage and / or cabinet at each IBX data center.	No exceptions noted.
CC6.4.11	The data center floor does not have windows leading to the exterior of the building, where applicable. In cases due to the existing infrastructure having windows and entry points leading to the exterior, then they need to be locked from inside or access controlled.	Observed the colocation space at the IBX data centers with the assistance of the data center site managers and security personnel to determine that the data center floor did not have windows leading to the exterior of the building or in cases due to the existing infrastructure having had windows leading to the exterior, those windows were locked from the inside or access controlled at each IBX data center.	No exceptions noted.
CC6.4.12	Physical access reviews are documented and approved by information security personnel at least annually for IBX data centers.	Inspected the most recently completed physical access review documentation for a sample of IBX data centers to determine that physical access reviews were documented and approved by information security personnel during the period for each IBX data center sampled.	No exceptions noted.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Asset removal and disposal policies are in place to guide personnel in the disposal of assets to ensure data and software is 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.5.2	Media containing sensitive data is securely wiped or destroyed prior to retiring a physical asset.	Inspected the completed disposal forms, certificates of destruction, and tracking documentation for a sample of physical media assets retired during the period to determine that the secure data removal or destruction activities were tracked for each retired asset sampled.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Firewalls are configured to filter unauthorized inbound network traffic from the Internet and deny network connections not explicitly authorized by a rule.	Inspected the global firewall ruleset and system generated listing of firewall devices managed via the centralized firewall management system to determine that firewall systems were configured to filter unauthorized inbound network traffic from the Internet and deny network connections not explicitly authorized by a rule.	No exceptions noted.
CC6.6.2	An IDS is utilized to monitor and analyze network traffic for possible or actual security breach events.	Inspected the IDS dashboard, threat detection configurations, and example threat event logs generated during the period to determine that an IDS was utilized to monitor and analyze network traffic for possible or actual security breach events.	No exceptions noted.
CC6.6.3	A zero trust network access solution is utilized to establish secure connections and is configured to enforce two-factor authentication requirements for access to the corporate network.	Inspected the zero trust network access solution user authentication and encryption policy configurations to determine that a zero trust network access solution was utilized to establish secure connections and was configured to enforce two-factor authentication requirements to the corporate network.	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: · Monthly network vulnerability assessments · Annual penetration testing for the customer web portal Remediation plans are proposed and monitored through resolution.	Inspected the network vulnerability assessment scanning tool configurations, results of monthly vulnerability scans completed during the period, and remediation documentation to determine that a network vulnerability assessment tool was configured to run monthly network vulnerability assessments performed and that remediation plans were documented and tracked through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent customer web portal penetration testing report and the corresponding remediation documentation to determine that penetration testing was performed for the customer web portal and that remediation plans were documented and tracked through resolution during the period.	No exceptions noted.
CC6.6.5	Access to the ECP requires users to authenticate via a user account and password and is configured to enforce minimum password requirements.	Inspected the ECP authentication configurations to determine that the ECP was configured to require users to authenticate via a user account and password and enforce minimum password requirements.	No exceptions noted.
CC6.6.6	ECP web servers utilize TLS 1.2 and TLS 1.3 encryption for web communication sessions.	Inspected digital certificates for the ECP web servers to determine that the ECP web servers utilized TLS 1.2 and TLS 1.3 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 and encryption 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	ECP web servers utilize TLS 1.2 and TLS 1.3 encryption for web communication sessions.	Inspected digital certificates for the ECP web servers to determine that the ECP web servers utilized TLS 1.2 and TLS 1.3 encryption for web communication sessions.	No exceptions noted.
CC6.7.3	A zero trust network access solution is utilized to establish secure connections and is configured to enforce two-factor authentication requirements for access to the corporate network.	Inspected the zero trust network access solution user authentication and encryption policy configurations to determine that a zero trust network access solution was utilized to establish secure connections and was configured to enforce two-factor authentication requirements to the corporate network.	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	Next generation antivirus/anti-malware software is configured to scan and monitor registered workstations and production endpoints in real time for abnormal and malicious behavior using behavioral analytics.	Inspected the enterprise antivirus software dashboard, prevention policy configurations, and listing of managed endpoints to determine that next generation antivirus/anti-malware software was configured to scan and monitor registered workstation and production endpoints in real time for abnormal and malicious behavior using behavioral analytics.	No exceptions noted.
CC6.8.2	A SIEM application is utilized to monitor and log certain security events for the in-scope systems when predefined conditions are met.	Inspected the SIEM application configurations, system-generated listing of monitored devices, and example security event logs generated during the period to determine that a SIEM application was utilized to monitor and log certain security events for the in-scope systems when predefined conditions were met.	No exceptions noted.
CC6.8.3	An IDS is utilized to monitor and analyze network traffic for possible or actual security breach events.	Inspected the IDS dashboard, threat detection configurations, and example threat event logs generated during the period to determine that an IDS was utilized to monitor and analyze network traffic 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 when predefined conditions are met.	Inspected the SIEM application configurations, system-generated listing of monitored devices, and example security event logs generated during the period to determine that a SIEM application was utilized to monitor and log certain security events for the in-scope systems when predefined conditions were met.	No exceptions noted.
CC7.1.2	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: · Monthly network vulnerability assessments · Annual penetration testing for the customer web portal Remediation plans are proposed and monitored through resolution.	Inspected the network vulnerability assessment scanning tool configurations, results of monthly vulnerability scans completed during the period, and remediation documentation to determine that a network vulnerability assessment tool was configured to run monthly network vulnerability assessments performed and that remediation plans were documented and tracked through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent customer web portal penetration testing report and the corresponding remediation documentation to determine that penetration testing was performed for the customer web portal and that remediation plans were documented and tracked through resolution during the period.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	A SIEM application is utilized to monitor and log certain security events for the in-scope systems when predefined conditions are met.	Inspected the SIEM application configurations, system-generated listing of monitored devices, and example security event logs generated during the period to determine that a SIEM application was utilized to monitor and log certain security events for the in-scope systems when predefined conditions were met.	No exceptions noted.
CC7.2.2	An IDS is utilized to monitor and analyze network traffic for possible or actual security breach events.	Inspected the IDS dashboard, threat detection configurations, and example threat event logs generated during the period to determine that an IDS was utilized to monitor and analyze network traffic for possible or actual security breach events.	No exceptions noted.
CC7.2.3	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis, including: · Monthly network vulnerability assessments · Annual penetration testing for the customer web portal Remediation plans are proposed and monitored through resolution.	Inspected the network vulnerability assessment scanning tool configurations, results of monthly vulnerability scans completed during the period, and remediation documentation to determine that a network vulnerability assessment tool was configured to run monthly network vulnerability assessments performed and that remediation plans were documented and tracked through resolution.	No exceptions noted.
		Inspected the most recent customer web portal penetration testing report and the corresponding remediation documentation to determine that penetration testing was performed for the customer web portal and that remediation plans were documented and tracked through resolution during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.4	Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.	Observed the surveillance camera systems and security monitoring procedures throughout the IBX data centers with the assistance of the data center site managers and security personnel to determine that internal and external monitoring of data center activity was performed through the use of security guard personnel and / or surveillance cameras at each IBX data center.	No exceptions noted.
		Inspected the security guard shift schedule for a sample of IBX data centers and months during the period to determine that security guard personnel were scheduled 24x7 to monitor data center activity for each IBX data center and month sampled.	No exceptions noted.
CC7.2.5	IBX facilities are monitored 24x7 by facilities engineers. Equinix has staff in place either onsite or on call 24x7 who are alerted by the BMS for system exceptions.	Inquired of the data center site managers and facilities personnel regarding the environmental security monitoring procedures to determine that the IBX data centers were monitored 24x7 by facility engineers and that Equinix had staff in place either onsite or on call 24x7 who were alerted by the BMS for system exceptions.	No exceptions noted.
		Inspected the site facility engineer staffing schedules for a sample of IBX data centers and months during the period to determine that facility engineers were scheduled 24x7 onsite or on call to monitor the facilities for each IBX data center and the dates during each month sampled.	No exceptions noted.
		Inspected the BMS monitoring dashboard and example alert log notifications generated during the period for a sample of IBX data centers to determine that a BMS was used to monitor the critical facility equipment and alert personnel when potential issues were identified for each IBX data center 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 management policies, procedures, and workflows 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	An enterprise ticketing system is utilized to document and track system security and availability incidents through resolution.	Inspected the system-generated listing of incident tickets logged in the ticketing system and the incident ticket details for a sample of incidents closed during the period to determine that an enterprise ticketing system was utilized to document and track system security and availability incidents through resolution for each incident sampled.	No exceptions noted.
CC7.3.3	A root cause analysis is determined for incidents that includes an impact analysis, action items, and where applicable, lessons learned.	Inspected the incident tickets for a sample of incidents closed during the period to determine that a root cause analysis was performed that included an impact analysis, action items, and where applicable, lessons learned for each incident sampled.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	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 management policies, procedures, and workflows 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.2	An enterprise ticketing system is utilized to document and track system security and availability incidents through resolution.	Inspected the system-generated listing of incident tickets logged in the ticketing system and the incident ticket details for a sample of incidents closed during the period to determine that an enterprise ticketing system was utilized to document and track system security and availability incidents through resolution for each incident sampled.	No exceptions noted.
CC7.4.3	A root cause analysis is determined for incidents that includes an impact analysis, action items, and where applicable, lessons learned.	Inspected the incident tickets for a sample of incidents closed during the period to determine that a root cause analysis was performed that included an impact analysis, action items, and where applicable, lessons learned for each incident sampled.	No exceptions noted.
CC7.4.4	Data center facility incidents and corrective measures are reported monthly for management review.	Inspected the security KPI reports for a sample of IBX data centers and months during the period to determine that reports addressing data center facility incidents and corrective measures were reported for management review for each IBX data center and month sampled.	No exceptions noted.
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 management policies, procedures, and workflows 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 determined for incidents that includes an impact analysis, action items, and where applicable, lessons learned.	Inspected the incident tickets for a sample of incidents closed during the period to determine that a root cause analysis was performed that included an impact analysis, action items, and where applicable, lessons learned for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.3	Incident response plan testing is performed on an annual basis at each site using simulated incidents to determine the incident response effectiveness and documents the results.	Inspected the most recently completed annual disaster recovery and incident management testing reports (pull-the-plug testing reports) for a sample of IBX data centers to determine that incident response plans were tested during the period for each IBX data center sampled.	The test of the control activity disclosed that annual disaster recovery and incident management (pull-the-plug) testing was not performed during the period for two of 39 IBX data centers sampled.
CC7.5.4	A crisis management team meeting is held on an annual basis to assess the team's ability to effectively respond to security incidents.	Inquired of the operations compliance manager regarding the crisis management procedures to determine that a crisis management team meeting was held on an annual basis to assess the team's ability to effectively respond to security incidents.	No exceptions noted.
		Inspected the global crisis management plan and most recently completed crisis management team meeting documentation and exercise assessment report to determine that a crisis management team meeting was held during the period.	No exceptions noted.
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	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 requesting, 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 period to determine that changes were authorized, tested when applicable, and approved for each change sampled.	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 configuration and maintenance changes implemented during the period to determine that a ticket system was utilized to document and track configuration and maintenance activities for each change sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.4	The production environment is logically segmented from the test environments.	Inspected the network IP address configurations for example production and testing environments to determine that the production environment was logically segmented from the test environments.	No exceptions noted.
CC8.1.5	A CRB meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming change projects that affect the system.	Inspected the CRB meeting documentation for a sample of weeks during the period to determine that a CRB meeting was held to discuss and communicate the ongoing and upcoming change 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 listings of users with the ability to implement infrastructure and application changes to the in-scope systems with the assistance of the senior infrastructure and information security engineers to determine that access privileges to promote changes into production were restricted to user accounts accessible by authorized personnel for each system sampled.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	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 assessment policies, procedures, standard risk assessment templates, and the business continuity program procedures 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.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 annual threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled 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 certificates of property insurance for a sample of countries where the in-scope IBX data centers reside to determine that insurance coverage was in place during the period for the IBX data center locations and equipment in each country sampled.	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 IBX data centers. 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 annual threat and risk assessments, mitigation tracking documentation, and evidence of management review for a sample of IBX data centers to determine that a risk assessment was performed during the period for each IBX data center sampled that considered risks associated with third-party providers accessing the IBX data centers and that risks were identified using a risk evaluation process and formally documented, along with activities, for management review.	No exceptions noted.
CC9.2.2	Signed agreements addressing information security and confidentiality obligations are required to be in place with vendors prior to sharing restricted information with the provider or providing access to IBX data centers.	Inquired of the operations compliance manager regarding the IBX data center vendor assessment procedures to determine that signed agreements addressing information security and confidentiality obligations were required to be in place with vendors prior to sharing restricted information with the provider or providing access to IBX data centers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the executed service level and nondisclosure agreements for a sample of the vendors to determine that signed agreements addressing information security and confidentiality obligations were in place for each vendor sampled.	No exceptions noted.
CC9.2.3	Operations and compliance personnel complete performance reviews on at least an annual basis to help ensure that the vendors are in compliance with the organization's requirements.	Inspected the most recently completed annual vendor management performance review documentation for a sample of active vendors to determine that operations and compliance personnel completed performance reviews during the period to help ensure that the vendors were in compliance with the organization's requirements for each vendor sampled.	The test of the control activity disclosed that annual vendor management performance reviews were not performed during the period for eight of 25 vendors sampled.

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 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 period for a sample of IBX data centers to determine that a BMS was used to monitor the critical facility equipment and alert personnel when potential issues were identified for each IBX data center 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 period to determine that resource utilization was tracked within a ticketing system and reported to IT operations personnel for review for each month sampled.	No exceptions noted.
A1.1.3	Interactive data visualization software and dashboards are utilized to review availability trends and forecast as compared to system commitments in real-time.	Inspected the Power BI interactive data visualization software dashboards and reports for a sample of months during the period to determine that interactive data visualization software and dashboards were utilized to review availability trends and forecast as compared to system commitments in real-time 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 IBX data centers with the assistance of the data center site managers and facilities personnel to determine that fire detection and suppression equipment was in place at each IBX data center.	No exceptions noted.
A1.2.2	Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.	Observed the inspection tags for a sample of hand-held fire extinguishers at the IBX data centers with the assistance of the data center site managers and facilities personnel to determine that scheduled maintenance was performed to help ensure fire extinguishers were working properly during the period for each fire extinguisher sampled.	No exceptions noted.
		Inspected the most recent fire detection and suppression equipment preventative maintenance reports for a sample of IBX data centers to determine that scheduled maintenance procedures were performed for the fire detection and suppression equipment during the period for each IBX data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.3	Power management equipment for each IBX is in place, which in addition to stand by generators, will include one or more of the following: · The mission critical electrical loads have redundant UPS or critical power supply systems · Distributed redundancy achieved through a reserve UPS system · Power management modules to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring, and control of power to the critical customer and Equinix computer loads	Observed the power management systems at the IBX data centers with the assistance of the data center site managers and facilities personnel to determine that power management equipment was in place at each IBX data center which included stand by generators and one or more of the following: · The mission critical electrical loads have redundant UPS or critical power supply systems · Distributed redundancy achieved through a reserve UPS system · Power management modules to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring, and control of power to the critical customer and Equinix computer loads	No exceptions noted.
A1.2.4	Scheduled maintenance procedures are performed to test and validate the operation of the power management systems.	Inspected the most recent UPS and generator preventative maintenance reports for a sample of IBX data centers to determine that scheduled maintenance procedures were performed for the power management systems during the period for each IBX data center sampled.	No exceptions noted.
A1.2.5	Temperature and humidity are monitored and the required temperature is maintained throughout the IBX facilities through the use of air conditioning and ventilation equipment.	Observed the HVAC equipment at the IBX data centers with the assistance of the data center site managers and facilities personnel to determine that air conditioning and ventilation equipment was in place to maintain the required temperature at each IBX data center.	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.	Inspected the most recent HVAC equipment preventative maintenance reports for a sample of IBX data centers to determine that scheduled maintenance procedures were performed for the HVAC equipment during the period for each IBX data center sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.7	IBX facilities are monitored 24x7 by facilities engineers. Equinix has staff in place either onsite or on call 24x7 who are alerted by the BMS for system exceptions.	Inquired of the data center site managers and facilities personnel regarding the environmental security monitoring procedures to determine that the IBX data centers were monitored 24x7 by facility engineers and that Equinix had staff in place either onsite or on call 24x7 who were alerted by the BMS for system exceptions.	No exceptions noted.
		Inspected the site facility engineer staffing schedules for a sample of IBX data centers and months during the period to determine that facility engineers were scheduled 24x7 onsite or on call to monitor the facilities for each IBX data center and the dates during each month sampled.	No exceptions noted.
		Inspected the BMS monitoring dashboard and example alert log notifications generated during the period for a sample of IBX data centers to determine that a BMS was used to monitor the critical facility equipment and alert personnel when potential issues were identified for each IBX data center sampled.	No exceptions noted.
A1.2.8	Backup systems are in place to perform scheduled and manual backups of IBX data and systems at predefined times.	Inspected the backup utility configurations, image backup archive, and example backup logs generated during the period for IBX data and systems at a sample of data center facilities to determine that backup systems were in place to perform scheduled and manual backups of IBX data and systems at predefined times.	No exceptions noted.
A1.2.9	Documented emergency procedures in the form of global IBX incident management policies and business recovery plans, reviewed and approved by management on an annual basis, are in place to provide guidance in the event of disruptions caused by an unexpected event.	Inspected the global IBX incident management and business continuity program policies, procedures, and plans to determine that documented emergency procedures were in place to provide guidance in the event of disruptions caused by an unexpected event and were reviewed and approved by management during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the IBX business recovery plans for a sample of IBX data centers to determine that a business recovery plan was in place to provide guidance in the event of disruptions caused by an unexpected event and was reviewed and approved by management during the period for each IBX data center sampled.	No exceptions noted.
	Digital Realty, Samsung SDS,BT Communications Ireland, and Khazna are responsible for ensuring that the facility environmental security controls for the colocation space, backup media storage, and other sensitive locations (including maintenance of sensitive system components within these locations) at the Chicago 4 (CH4), Seoul 1 (SL1),Dublin 1 (DB1), Dubai 2 (DX2) and Abu Dhabi (AD1) data center facilities are designed, monitored, and operating effectively.		
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 centers to determine that scheduled maintenance procedures were performed on environmental systems during the period at each IBX data center 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 recently completed annual disaster recovery and incident management testing reports (pull-the-plug testing reports) for a sample of IBX data centers to determine that disaster recovery testing was performed during the period for each IBX data center sampled.	Refer to the test results for control activity CC7.5.3.
	Digital Realty, Samsung SDS,BT Communications Ireland, and Khazna are responsible for ensuring that the facility environmental security controls for the colocation space, backup media storage, and other sensitive locations (including maintenance of sensitive system components within these locations) at the Chicago 4 (CH4), Seoul 1 (SL1),Dublin 1 (DB1), Dubai 2 (DX2) and Abu Dhabi (AD1) data center facilities are designed, monitored, and operating effectively.		

SECTION 5

OTHER INFORMATION PROVIDED BY EQUINIX

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Security and Availability

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.3	Incident response plan testing is performed on an annual basis at each site using simulated incidents to determine the incident response effectiveness and documents the results.	Inspected the most recently completed annual disaster recovery and incident management testing reports (pull-the-plug testing reports) for a sample of IBX data centers to determine that incident response plans were tested during the period for each IBX data center sampled.	The test of the control activity disclosed that annual disaster recovery and incident management (pull-the-plug) testing was not performed during the period for two of 39 IBX data centers sampled.
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 recently completed annual disaster recovery and incident management testing reports (pull-the-plug testing reports) for a sample of IBX data centers to determine that disaster recovery testing was performed during the period for each IBX data center sampled.	
Management's Response:	The two IBX data centers (FR6 and ST4) identified in this exception were undergoing critical infrastructure replacement and upgrade works which made it operationally impractical to conduct the tests during the scope period. Following successful completion of the works, the tests were promptly conducted at both IBX data centers in November 2024 with no issues identified.		

Security

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.3	Operations and compliance personnel complete performance reviews on at least an annual basis to help ensure that the vendors are in compliance with the organization's requirements.	Inspected the most recently completed annual vendor management performance review documentation for a sample of active vendors to determine that operations and compliance personnel completed performance reviews during the period to help ensure that the vendors were in compliance with the organization's requirements for each vendor sampled.	The test of the control activity disclosed that annual vendor management performance reviews were not performed during the period for eight of 25 vendors sampled.
Management's Response:	Equinix can confirm that annual vendor performance reviews for the 8 vendors identified have been initiated as of November 2024. Additionally, Equinix has implemented a robust process to ensure compliance with annual vendor performance review requirements going forward. Equinix has also integrated vendor performance review checks into their regular internal audit program to ensure reviews are completed as required.		

EQUINIX'S GLOBAL DATA PRIVACY POSITIONING STATEMENT

This is a positioning statement in relation to data privacy and how Equinix, as a global organization, manages compliance with data privacy laws around the world that regulate the handling and controlling of personal data. Equinix is a global operator of high availability data centers, providing colocation, interconnection, and ancillary services (collectively described as "data center services") to enterprises around the world. Equinix operates a Global Privacy Program built on a privacy by design and default framework, demonstrating a commitment to industry leadership and best practices for both our customers and internal operations.

Equinix's Guiding Principles

We are committed to complying with all applicable laws wherever Equinix does business. Equinix's policies reflect its commitment to fair and transparent data handling practices. We do this by:

i. Acting in compliance with relevant laws and regulations at the global, regional, or local levels in all locations where we operate. Equinix regularly monitors the external environment and updates its practices in response to new requirements or changes in the laws of the countries in which it operates. Equinix has taken advice from its internal and external legal advisers in designing and implementing its Global Privacy Program;

ii. Collecting only the personal data relevant to conduct our business, and processing and storing it in accordance with our established policies and procedures;

iii. Helping individuals understand how their personal data will be collected and used when interacting with Equinix; and

iv. Maintaining appropriate security systems for the processing of personal data, supported by encryption, anonymization, and other measures to protect against unauthorized access or disclosure. Equinix's measures align with industry standards, such as NIST and ISO series.

Equinix's relationship with personal data

Equinix acts as a data controller (per Article 4(7) of the European General Data Protection Regulation 2016/679 ("GDPR")) with respect to the processing of certain personal data it handles on its prospects, customers, visitors to its premises and website, vendors, and employees. As the data controller, Equinix determines both the purposes and the means for processing in the context of the overall business or employment relationship. Consequently, Equinix is directly responsible for ensuring that such personal data is adequately protected when collected, used and/or transferred from one country to another.

In this respect, Equinix's collection, processing, storage, and transfer of personal data is carried out in accordance with the Equinix Privacy Statement and designed for compliance with:

i. Global and Regional Data Protection Laws: Equinix complies with data protection laws in all relevant jurisdictions where it operates, including but not limited to the GDPR, the E-Privacy Directive 2002/58/EC, the UK GDPR, the California Consumer Privacy Act ("CCPA"), the Brazilian General Data Protection Law ("LGPD"), and the Personal Data Protection Act ("PDPA") in Singapore. Equinix monitors global regulatory developments to ensure its practices remain aligned with evolving laws and standards.

ii. Binding Corporate Rules ("BCRs") and Standard Contractual Clauses ("SCCs"): Equinix's BCRs under the GDPR and UK GDPR facilitate the secure transfer of personal data from the European Economic Area ("EEA"), Switzerland, and UK to its affiliates worldwide whilst adhering to the highest standards required by the data protection regulators in these jurisdictions. In other regions, Equinix uses lawful mechanisms such as SCCs and approved intra-group agreements.

iii. Global Standards and Regulatory Expectations: Equinix adheres to international standards for data protection and transfer, guided by entities such as the European Data Protection Board ("EDPB"), the Federal Trade Commission ("FTC") in the U.S., Brazil's National Data Protection Authority ("ANPD"), Singapore's Personal Data Protection Commission ("PDPC"), and other national regulators to ensure that

appropriate legal and other safeguards are in place for the handling of personal data both within and outside of the Equinix affiliated group of companies.

A "gold standard" Global Privacy Program

Equinix's Global Privacy Program is designed to ensure the responsible handling of personal data in accordance with the most rigorous data privacy laws and standards worldwide. By embedding strong privacy principles across our operations, Equinix ensures that personal data is managed consistently and securely, irrespective of geographic location.

Historically, Equinix has used the SCCs in its inter-company agreements to facilitate data transfers from the UK, EEA, and Switzerland. However, the BCRs provide the added "gold standard" by ensuring adequate safeguards for intra-group transfers, supporting both operational needs and the seamless flow of data necessary to run a global enterprise. This endorsement from the EU for our transborder data flows is foundational for our own compliance strategy and assisting our global customers with theirs.

We also implement other contractual, technical, and organizational safeguards to meet the varying requirements of other global privacy laws outside of Europe. Our continuous assessment of data transfer risks, which we monitor regardless of the origin of the transfer, ensures that where necessary, we implement additional safeguards to mitigate risks. Equinix's corporate position prioritizes data privacy and the general integrity of personal and enterprise data.

Equinix services and personal data

Equinix's clear position is that in the context of its data center services:

i. As Equinix (and/or its agents, representatives, suppliers or sub-contractors) has no physical or logical access to, use of, or control over, nor performs any processing activity on, or assumes any responsibility for the customer or end-user application data that transits or is stored on customer-owned or controlled server equipment ("End-User Data") (refer to our Shared Responsibility Model), such End-User Data falls outside the scope of data privacy legislation applicable to Equinix's business and its Global Privacy Program. As a result, Equinix does not perform any processing activity and does not assume any legal responsibility as a data processor (or data controller or otherwise) in relation to the End-User Data; and

ii. Equinix's customers remain responsible as data controllers in relation to End-User Data and as such, are solely responsible for their compliance with applicable data privacy laws globally. The only personal data for which Equinix assumes responsibilities are: (i) contact details and related personal data, including account information that Equinix uses to provide its services, as further detailed in the Equinix Privacy Statement; and (ii) biometric data, provided by customer representatives for authentication when accessing our secure IBX data centers. Equinix handles this personal data in compliance with applicable data protection regulations, and the manages customer relationships through its global CRM database.

Global law compliance and on-going maintenance of the Global Privacy Program

Equinix reviews global data privacy laws and regulations as they apply to its business and its Global Privacy Program, ensuring compliance in the markets in which it operates. This includes staying current regarding ongoing judicial, regulatory, and other authoritative interpretations and guidance.

A growing number of governments are implementing data privacy regulations, including regions where Equinix operates, such as California, Brazil, Singapore, and India. Equinix's Global Privacy Program is a critical element of its broader compliance framework, supporting our global customers and partners who rely on us for secure and trustworthy operations. We continuously review our program to remain at the forefront of global privacy compliance.

This positioning statement is not to be taken or understood as legal advice or opinion by Equinix, and may be updated periodically in response to organizational, legal, or business changes that may take place.