

EQUINIX

SOC I REPORT

FOR

AMERICAS DATA CENTER HOSTING AND BRASIL MANAGED SERVICES

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

FOR THE PERIOD NOVEMBER 1, 2019, TO OCTOBER 31, 2020

PREPARED IN ACCORDANCE WITH THE
AICPA SSAE No. 18 AND IAASB ISAE 3402 STANDARDS

Attestation and Compliance Services



Proprietary & Confidential

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

This report is intended solely for use by the management of Equinix, Inc., its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a "specified user").

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

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

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	5
SECTION 3	DESCRIPTION OF THE SYSTEM	8
SECTION 4	TESTING MATRICES	36
SECTION 5	OTHER INFORMATION PROVIDED BY MANAGEMENT	57

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Equinix, Inc.:

Scope

We have examined Equinix, Inc.'s ("Equinix" or "service organization") description of its Americas Data Center Hosting Services and Brasil Managed Services system throughout the period November 1, 2019, to October 31, 2020 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of Equinix believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Americas Data Center Hosting Services and Brasil Managed Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Equinix's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Equinix uses a subservice organization for all of the environmental protection controls at the Chicago 4 (CH4) data center facility and all of the physical security controls at the Dallas 10 (DA10) data center facility. The description includes only the control objectives and related controls of Equinix and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified by Equinix can be achieved only if complementary subservice organization controls assumed in the design of Equinix's controls are suitably designed and operating effectively, along with the related controls at Equinix. Our examination did not extend to controls of the subservice organization, 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 Management" is presented by management of Equinix to provide additional information and is not a part of Equinix's description of its Americas Data Center Hosting Services and Brasil Managed Services system made available to user entities during the period November 1, 2019, to October 31, 2020. Information in Section 5 has not been subjected to the procedures applied in the examination of description of the Americas Data Center Hosting Services and Brasil Managed Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Americas Data Center Hosting Services and Brasil Managed Services system.

Service Organization's Responsibilities

In Section 2, Equinix has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Equinix is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives 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 International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2019, to October 31, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Control

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

We applied the Statements on Quality Control 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 user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in providing the data center hosting services and managed services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

Opinion

In our opinion, in all material respects, based on the criteria described in Equinix's assertion in Section 2,

- a. the description fairly presents the Americas Data Center Hosting Services and Brasil Managed Services system that was designed and implemented throughout the period November 1, 2019, to October 31, 2020;
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2019, to October 31, 2020, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of Equinix's controls throughout the period November 1, 2019, to October 31, 2020; and
- c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2019, to October 31, 2020, if, as applicable,

complementary subservice organization and user entity controls assumed in the design of Equinix's controls operated effectively throughout the period November 1, 2019, to October 31, 2020.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of Equinix, user entities of Equinix's Americas Data Center Hosting Services and Brasil Managed Services system during some or all of the period November 1, 2019, to October 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

SCHULMAN & COMPANY, LLC

Tampa, Florida
December 8, 2020

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of Equinix, Inc.'s ("Equinix") Americas Data Center Hosting and Brasil Managed Services system throughout the period November 1, 2019, to October 31, 2020 (the "description"), for user entities of the system during some or all of the period November 1, 2019, to October 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

Equinix uses a subservice organization for all of the environmental protection controls at the Chicago 4 (CH4) data center facility and all of the physical security controls at the Dallas 10 (DA10) data center facility. The description includes only the control objectives and related controls of Equinix and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Equinix's controls are suitably designed and operating effectively, along with related controls at Equinix. The description does not extend to controls of the user entities.

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

- a. the description fairly presents the Americas Data Center Hosting and Brasil Managed Services system made available to user entities of the system during some or all of the period November 1, 2019, to October 31, 2020, for providing data center hosting services as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, as applicable:
 - (1) the types of services provided including, as appropriate, the classes of transactions processed;
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities of the system;
 - (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;
 - (4) how the system captures and addresses significant events and conditions, other than transactions;
 - (5) the process used to prepare reports or other information provided for entities;
 - (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;
 - (7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the Equinix's controls; and

- (8) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided;
 - ii. includes relevant details of changes to the Americas Data Center Hosting and Brasil Managed Services system during the period covered by the description; and
 - iii. does not omit or distort information relevant to the scope of the Americas Data Center Hosting and Brasil Managed Services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Americas Data Center Hosting and Brasil Managed Services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period November 1, 2019, to October 31, 2020, to achieve those control objectives if, as applicable, subservice organizations and user entities applied complementary controls assumed in the design of Equinix's controls throughout the period November 1, 2019, to October 31, 2020. The criteria we used in making this assertion were that
- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of Equinix;
 - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Equinix was founded in 1998 and operates International Business Exchange™ (IBX) data centers offering businesses a place to run their operations and exchange information. Equinix's interconnection platform spans 63 markets on five continents and hosts a comprehensive portfolio of digital services and ecosystems that allows customers to securely scale their digital infrastructure wherever opportunity leads. More than 9,500 companies populate Equinix's diverse ecosystems, and all are potential partners or customers.

Description of Services Provided

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

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

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

Other security features and controls may include:

- Control points between exterior and customer equipment
- Weekly cross-IBX security meetings
- Customer self-administration of authority levels for ordering and access
- Segregation of order management (done by customer service and/or sales) and service delivery functions in order to assure no "local agreements"
- Customer privacy policies, including no pictures and customer anonymity

- Facility design, which includes controlled access points, reinforced exterior walls
- Token authentication required for access to enterprise network
- Bullet-resistant protection
- Motion-detection lighting, and automatic lighting that activated in the event of a power outage or disruption including facility emergency exits

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

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

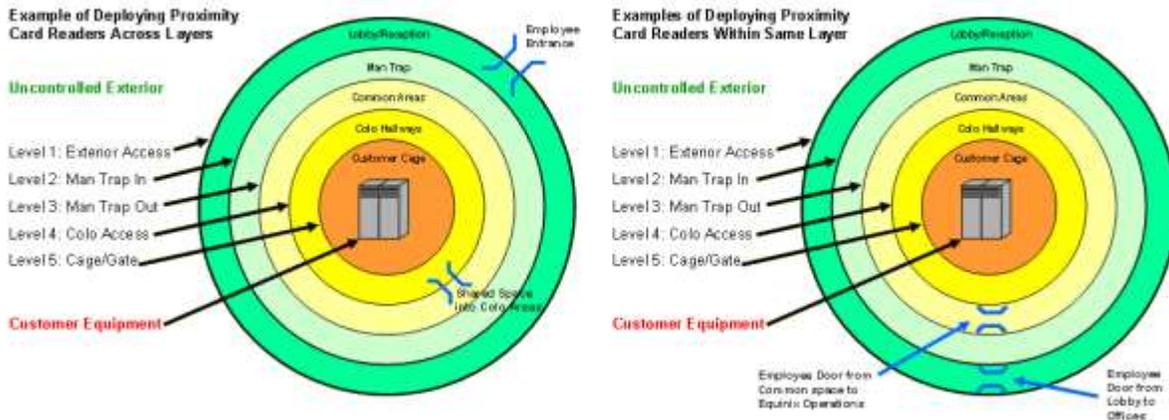
The LA2 IBX facility was not constructed by Equinix. Size constraints limited the amount of remodeling that could be accomplished, and exceptions were allowed in the redesign. The LA2 facility has one biometric hand scan reader located at the entrance to the site. Instead of a mantrap, security officers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

Employee Data Center Access

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

The Siebel ticketing system is a web-based portal that security personnel use to view requests for access, access enrollment authorization, and removal, etc. The data written into the log and notes section of a SR is used to update the status of the SR. Proximity card issuance and biometric profile setup and modification activities are performed by security personnel only upon receipt of an access enrollment requests ticket, which indicates the person is an authorized Equinix employee or contractor. Personnel authorized to work at an Equinix facility are required to display ID badges when entering or working within an Equinix IBX. Depending on the access privileges, off-site employees may be required to be escorted by authorized personnel while within the facility.

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



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

Customer Data Center Access

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

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

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

Vendor and Contractor Data Center Access

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

Visitor Data Center Access

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

Physical Access Removal

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

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

Security Personnel Formal Training

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

- Equinix company overview
- Safety training videos and/or classes
- Walkthrough of the IBX and orientation of the various equipment
- Security officer responsibilities, including assigning access and access enrollment procedures
- Security systems walkthrough of access control
- Response to emergencies, including fire alarms, bomb threats, and other natural disasters and evacuation procedures
- Incident reporting
- Site-specific procedures

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

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

Facility and Environmental Protection

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

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

IBX facilities meet applicable state, local and federal regulatory requirements for environmental health and safety, including written emergency response plans, emergency contacts notification, inventory of hazardous chemicals, personal protective equipment, chemical spill kits, and hazard communication/warning signage. Emergency standard operating procedures contain documentation about the emergency procedures that address fires, bombs

threats, severe weather, and medical emergencies. Other policies and procedures are in place to help ensure that IBX facilities have a consistent level of facility and environmental protection.

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

Control and Monitoring Systems

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

This BMS system monitors/controls the following:

- Power systems, including critical electrical components, generators, transfer switches, main switchgears, power distribution units (PDUs), automatic static transfer switches (ASTS), and UPS equipment;
- The HVAC system, which controls and/or monitors space temperature and humidity within the IBX facilities, space pressurization, HVAC equipment status and performance, and outside air conditions;
- Fire detection and suppression equipment, such as very early smoke detection apparatus (VESDA), double interlock pre-action and detection systems, and zoned gaseous-based fire extinguishing system; and
- Leak detection systems.

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

Fire Detection and Suppression

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

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

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

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

The fire suppression system is monitored on a 24-hour basis by an external alarm monitoring company, which will dispatch the city fire department upon receipt of an alarm. Inside the IBX facilities, software is used for fire detection

and monitoring, combined with customized floor plan graphics to illustrate detection devices and fire zones to aid IBX personnel and the fire department in responding to and coordinating fire control activities.

Power Management Utility and Backup Power

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

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

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

The mission critical electrical loads at each IBX facility are sourced by redundant static or rotary UPS systems, which are configured with automatic static bypass and manually operated full maintenance bypass circuits. The primary UPS systems operate as an online power supply. The UPS systems provide conditioned, uninterruptible power to critical electrical loads. Customer critical loads are protected by an alternate UPS through the use of ASTS. Web-based reporting services monitor UPS batteries and provide regular battery-automated reporting analysis to the sites that measures the impedance of each jar in a UPS battery system. Impedance trends are used to monitor the health of each jar and to assist in replacement scheduling. The system is also used to monitor ambient temperature of the battery rooms/cabinets in order to verify proper environmental conditions.

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

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

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

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

HVAC

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

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

- Condenser pumps
- Centrifugal chillers
- Cooling towers

- Primary chilled water pumps or air-cooled condensers
- Air handling units in the collocation area

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

Leak Detection System

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

Maintenance of Critical Systems

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

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

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

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

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

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

Brasil Managed Services

Brasil’s data center sites 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. The following core services are provided to managed services customers:

- Power availability: power and cooling equipment for collocation areas
- Redundancy: 2N and N+1 redundancy for UPS units, generators, power distribution, and cooling
- Safety: environmental control monitoring and alerts, dry pipe fire suppression system

- Security: 24 hours per day security management and site access
- Service: centralized command and control of standard process and procedures across sites

Within the colocation facilities, cabinet locations feature direct access to the data distribution system to allow quickly deployable interconnections. Equinix personnel can recommend cages and suites to meet specific requirements for physical security and power usage. Private and shared cages are configured with cable distribution systems, dual alternating current (AC) and direct current (DC) power distribution raceways, and anonymous cabinets (individually locked if necessary). Private and shared suites are also available at select locations, providing a fully enclosed, customized area.

Dedicated Servers and Hardware

Within this service offering, Equinix provides equipment in conjunction with the colocation service for its customers. Equinix's provided equipment is hosted on the data center premises, according to the contracts setup with customers.

Connectivity

Equinix's connectivity service offering provides access to the public internet for customer equipment hosted at Equinix Data Centers.

Hosting Management

Hosting management services consist of providing labor force and specialized resources to run planned or as needed activities pertaining to the operation of servers and network devices of customers hosted at Equinix Data Centers.

Help Desk

Customer's utilizing this service may open tickets, through the customer portal or help desk, for the Equinix team to provide technical support for installation, operation, change of setup or recovery from failure in servers or network devices hosted by Equinix.

Total Management (Partial Outsourcing)

This service includes help desk and disaster recovery functions. For this service offering, the Equinix team is responsible for the installation, operation, maintenance, security, monitoring and updates to the setup of the hardware, operating system, database and applications of customer equipment. Activities/Changes can be scheduled or run on an as needed basis, through a ticket request that customer will open through Equinix Customer Portal. Based on the ticket received Equinix team will perform related activities/changes and interact with customers through the ticketing system

Dedicated Leader

The dedicated leader service consists of technical and management resources during business hours. Dedicated leader resources perform technical and management functions for the equipment hosted by Equinix.

Initiation, Authorization, Recording, Processing, Correction, and Transferring of Information to Customers

The services that Equinix provides for its clients described in the description of its system and the scope definition below enable Equinix customers to host their production systems at Equinix's data centers. Equinix plays no role in the initiation, authorization, recording, processing, and correction or transferring of information to its clients, outside of the processes, described above, that relate to Equinix's information technology general controls for the data center hosting services.

Customer requests for services are initiated and authorized by user entities by directly contacting the customer support department. Customer requests are recorded and track within the ServiceNow internal ticketing system through resolution. The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established service level agreements.

Boundaries of the System

The scope of the review includes the Americas Data Center Hosting Services performed at each of the data center facilities listed below, and the Brasil Managed Services performed at the Rio de Janeiro (RJ1 and RJ2), São Paulo (SP1), Tamboré (SP2, SP4), and Santana de Parnaíba (SP3) data center facilities. Additionally, the support and management functions of the Tampa, Florida, field office (TPFO) relevant to the Americas Data Center Hosting Services were included within the scope of the review. The control objectives and related control activities included within the scope of this engagement can be found in Section 4. The Americas Data Center Hosting Services are limited to the Physical and Environmental Security control objectives and related control activities identified in Section 4 of this document. The other control objectives and related control activities provided in Section 4 are for specific to the Brasil Managed Services.

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

Location	Site
Atlanta, Georgia	AT1, AT2, AT3, AT4, AT5
Boston, Massachusetts	BO2
Chicago, Illinois	CH1, CH2, CH3, CH4*, CH7
Culpeper, Virginia	CU1, CU2, CU3, CU4
Dallas, Texas	DA1, DA2, DA3, DA4, DA6, DA7, DA9, DA10**, DA11***
Denver, Colorado	DE1, DE2
Houston, Texas	HO1
Los Angeles, California	LA1, LA2, LA3, LA4, LA7
Miami, Florida	MI1, MI2, MI3, MI6
New York, New York	NY1, NY2, NY4, NY5, NY6, NY7, NY8, NY9, NY11, NY13
Philadelphia, Pennsylvania	PH1
Seattle, Washington	SE2, SE3, SE4
Silicon Valley, California	SV1, SV2, SV3, SV4, SV5, SV6, SV8, SV10, SV13, SV14, SV15, SV16, SV17
Tampa, Florida	TPFO
Washington, D.C.	DC1, DC2, DC3, DC4, DC5, DC6, DC7, DC10, DC11, DC12, DC13, DC14, DC15***, DC97
Toronto, Ontario	TR1, TR2
Mexico City, Mexico	MX-1
Monterrey, Mexico	MO1
Bogotá, Colombia	BG1
Rio De Janeiro, Brazil	RJ1, RJ2
São Paulo, Brazil	SP1, SP2, SP3, SP4

*Physical only

**Environmental only

***The DA11 data center was placed into service on July 23, 2020. The testing of operating effectiveness of the control activities specific to DA11 were excluded from the scope of this report for the period November 1, 2019 through July 23, 2020 (the period prior to the service go-live date for DA11). The DC15 data center was placed into service on January 1, 2020. The testing of operating effectiveness of the control activities specific to DC15 were excluded from the scope of this report for the period November 1, 2019, through December 31, 2019 (the period prior to the service go-live date for DC15). As a result of the go-live date for the DA11 data center facility the

following control activity did not occur during the reporting period for DA11: Physical access system logs are recorded and maintained for a minimum of six months.

Equinix’s Americas Data Center Hosting and Brasil Managed Services system environment is an information technology (IT) general control system, and user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within Americas Data Center Hosting and Brasil Managed Services system; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Equinix utilizes the environmental protection services at the Chicago 4 (CH4) data center facility, and the physical security services at the Dallas 10 (DA10) data center facility services provided by Digital Realty Trust, Inc. (Digital Realty Trust). Equinix’s Americas Data Center Hosting Services and Brasil Managed Services system is designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the control objectives related to Equinix’s Americas Data Center Hosting Services and Brasil Managed Services system to be solely achieved by Equinix’s control activities. Accordingly, subservice organizations, in conjunction with the Americas Data Center Hosting Services and Brasil Managed Services system, should establish their own internal controls or procedures to complement those of Equinix.

Complementary Controls at Subservice Organizations

The following complementary subservice organization controls should be implemented by subservice organizations to provide additional assurance that the specified control objectives described within this report are achieved:

Control Activities Expected to be Implemented at Subservice Organization	Related Control Objective
Digital Realty Trust is responsible for ensuring that physical access to the Dallas 10 (DA10) data center facility (including colocation space, backup media storage and other sensitive locations as well as sensitive system component within this locations) is restricted authorized personnel.	Physical Security
Digital Realty Trust is responsible for the environmental protection controls design, development, implementation, operations, maintenance, and monitoring to meet availability commitments and requirements at the Chicago 4 (CH4) data center facility.	Environmental Security

Significant Changes During the Reporting Period

The DA11 data center was placed into service on July 23, 2020, and the DC15 data center was placed into services on January 1, 2020.

Also, on January 9, 2020, Equinix announced the completion of its acquisition of three data centers from Axtel S.A.B. de C.V. that serve the Mexico City and Monterrey metro areas of Mexico. Additionally, on October 1, 2020, Equinix announced the completion of its acquisition of 13 data centers in Canada and their operations from BCE Inc. (Bell Data Centers). No other significant changes to the Americas Data Center Hosting and Brasil Managed Services systems occurred during the reporting period.

No other significant changes to the Data Center Hosting Services system occurred during the reporting period.

Functional Areas of Operations

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

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

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

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.

Infrastructure and Software

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

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

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

Primary Infrastructure			
Production Application	Business Function Description	Operating System	Physical Location
Physical access control systems (various platforms – varies by region / location)	Biometric, proximity card, and/or personal identification number (PIN) reader system (varies by data center facility) used to restrict data center access to only those individuals provisioned with access; the systems are also used to monitor, log, and notify personnel of physical security alarms	Windows / Linux	Data center facilities / Equinix Operations Center (EOC)
CCTV system (various platforms – varies by region / location)	Surveillance camera system used for security monitoring of data centers 24 hours per day; CCTV cameras are positioned throughout the data centers to monitor and track the activity of any person while inside and outside of the data centers	Windows / Linux	Data center facilities / EOC
BMS (various platforms – varies by region / location)	Building management system used to monitor environmental controls and alert data center personnel to potential issues within the data center, including critical electrical components, power management equipment, heating, ventilation, and air-conditioning (HVAC) equipment, and fire detection and suppression equipment	Windows / Linux	Data center facilities / EOC

Primary Infrastructure			
Production Application	Business Function Description	Operating System	Physical Location
ECP	Web-based portal used by customers to manage their access control lists including access change requests and visitor access requests to data center; place orders for IBX data center products and schedule services; and view order statuses, access reports, account information, and review invoices	Windows / Linux	Corporate IT / Network Operations Center (NOC)
GSD and Siebel ticketing systems	Ticketing system used to record, track, and monitor internal and external reported incidents, requests, and notifications applicable to physical and environmental security matters	Windows / Linux	Data center facilities / EOC
IBM Maximo	Enterprise asset management system used to inventory and track assets for the IBX data center, as well as to schedule preventive and predictive maintenance work visits, issue work ticket, track costs, and records maintenance history	Windows / Linux	Data center facilities / EOC
Microsoft Active Directory (AD)	Directory services used to manage user accounts, access, and authentication requirements	Windows	Corporate IT / NOC
Firewalls, VPN gateways, routers, and switches	Corporate IT managed network devices and systems utilized to restrict, filter, and route traffic for Equinix's corporate network; VPN gateways Network devices used to facilitate secure connectivity to the Equinix corporate for data centers (site-to-site) and end users (point-to-point)	Palo Alto / Juniper / Cisco / Opengear / Avocent	Corporate IT / NOC
File storage systems	Disk storage devices used to present files and directories to local host and to hosts over the network	Windows / Linux	Corporate IT / NOC / Data center facilities

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

Data Management

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

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

- Biometrics, proximity card, and PIN code access history logs, including access history and security alarms
- CCTV recorded footage is maintained for 90 days, and at minimum 30 days
- Alert notifications and monitoring reports generated from the environmental monitoring applications, the BMS, and status of backup job completion.

- Incident/issue reports documented via the ticketing systems
- Enterprise monitoring applications are utilized to monitor the performance and availability of production servers and network infrastructure.

CONTROL ENVIRONMENT

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

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Equinix's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Equinix's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of Equinix's values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Equinix has implemented in this area are described below.

- Equinix's code of conduct is included within the employee manual 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.

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

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 security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- Management documents performance policies to align internal control responsibilities, performance measures and incentives with company business objectives.
- Management conducts a performance review of employees on an annual basis to evaluate individual performance against expected levels of performance and conduct.

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.

RISK ASSESSMENT

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the services organizations systems. 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. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

Risk Identification

Equinix considers the needs and expectations of interested parties and the boundaries of its data center hosting services system, which includes the identification and analysis of risks that pose a threat to the organization's ability to provide reliable services to its customers. The first step of the process is determining the organization's objectives is an essential part of the process and understanding the potential threats and vulnerabilities that could the threaten its ability to achieve said objectives. Equinix's the process focuses on supporting management decisions and

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

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

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

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

Risk Analysis

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions

about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Control Objectives and Related Control Activities section below. Additionally, management reviews the assessed risk levels on an annual basis and documents the risk assessment in the annual risk program. The risk assessment process includes a systematic approach of estimating the magnitude of risks and the process of comparing the estimated risks against risk acceptance criteria. The approach is comprised to three overarching components: risk identification, risks analysis/evaluation, and risk mitigation; to ensure repeatable risk assessment procedures that produce consistent, valid, and comparable results.

Risk Acceptance Criteria

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

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

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

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

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

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

Value	Probability (P)	Human Impact (HI)	Property Impact (PI)	Business Impact (BI)
0	Not applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0
1	Improbable occurrence – could not conceivably happened or expect to happen less than once in 100 years.	Negligible – no first aid required	Negligible – negligible damage	Negligible – no direct damage to business delivery (US\$0-\$135 / €0-100)
2	Possible occurrence – expected to happen once or more every 10 years (<i>Note: Includes 1 – 10 years</i>).	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-\$1,350,000 / €100,000-1,000,000)
6	Common occurrence – could happen daily / weekly.	Catastrophic – multiple deaths and/or serious injuries	Catastrophic – almost total damage or loss; facility must be torn down and replaced	Catastrophic – no business delivery possible (>US\$1,350,000 / €1,000,000)

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

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

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

The level of risk determined for each hazard is indicated in each region and/or country's IBX's threat and risk assessment survey register. The results of risk calculation are compared with the risk criteria established to prioritize the calculated risks for risk treatment. During the risk evaluation process, the appropriate risk treatment option is selected and all controls that are necessary to implement the information security risk treatment option are chosen. Each risk treatment plan is assigned a risk owner, and the risk owner provides their approval of the risk treatment plan by formally reviewing the risk assessment which details the risk treatment plan(s). Evidence of these approvals is retained in the risk assessment spreadsheet. The key control matrix is updated and the risk treatment plan is documented. The risk owners' approval for the risk treatment plan is received. Once the risk treatment has been completed, the risk owners accept any residual risk.

Integration with Control Objectives

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

Control activities are a part of the process by which Equinix strives to achieve its business objectives. Equinix has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of Equinix evaluate the relationships between business processes and the use technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Equinix personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed and improved when necessary.

Equinix's control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. 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.

Physical Security

Control Objective: Control activities provide reasonable assurance that physical access to Equinix locations, facility infrastructure platforms, and customer's footprints(s) is limited to properly authorized individuals.

Each of the Equinix data center facilities adhere to structured processes and procedures that ensure user entities technology assets are secure. The data center facilities are manned by on-site technical experts 24 hours per day to help ensure equipment that supports that data center environment is secure. In addition, Equinix employs a training program to help ensure that Equinix data center personnel are trained in data center operations and security.

Equinix data center facilities incorporate multiple physical and operational security features and protocols including the following: biometric fingerprint readers, badge access card, PIN access, and CCTV surveillance with video stored for review for non-repudiation, multifactor authentication systems, and staff trained to maintain physical security policies and controls, perimeter doors that are alarmed and monitored. CCTV surveillance cameras are in place to monitor and record activity at the entrance to and throughout the data center facilities.

There are processes in place to log access to the data center facilities by authorized users and employees. Visitors are required to present government issued identification and to be provided with escorted access within the data center facilities. Access to the colocation areas requires a valid badge access card. Both successful and unsuccessful badge access attempts are tracked in the badge access system. Management provisions badge access privileges as a component of the employee hiring process. Management revokes badge access privileges as a component of the employee termination process. Access to the colocation areas requires a valid badge access card. Administrator access within the badge access system is restricted to user accounts accessible by authorized personnel. The exterior walls extend from the floor to the ceiling.

Environmental Security

Control Objective: Control activities provide reasonable assurance that Equinix facilities housing customer equipment and support operations are engineered and monitored to reduce the risk of environmental threats (i.e., power loss, fire, and flooding).

Equinix has implemented and documented policies and procedures to ensure the environmental security of the data center facilities. Equinix data centers incorporate cooling solutions to ensure consistent temperature and humidity levels for the protection of technology. The data center facilities are also equipped with raised floor cooling with cold aisle containment. In addition, facility components e.g. power generators and UPS systems throughout the data centers are redundant to provide continuous power in the event of an outage.

The data center facilities are also equipped with fire and smoke detectors which trigger visible and audible alarms in the event of a fire. A BMS is in place to monitor environmental conditions for data center facilities that include temperature and humidity levels. The data center facilities are equipped with multiple air conditioning units to regulate temperature and humidity.

Facilities personnel inspect the hand-held fire extinguishers, UPS, air conditioners, power generators, temperature and humidity levels on a periodic basis. Additionally, management contracts a third-party vendor to inspect the fire suppression systems, fire extinguishers, UPS, air conditioners, and power generators on an annual basis. Documentation of internal and external inspections is retained.

The following control objectives and processes are applicable to the Brasil Managed Services performed at the Rio de Janeiro (RJ1 and RJ2), São Paulo (SP1), Tamboré (SP2 and SP4), Santana de Parnaíba (SP3), and Brasil data center facilities only.

New Customer Implementation

Control Objective: Control activities provide reasonable assurance that new customers are implemented in line with contractual requirements.

New customer implementations for Equinix follow a standard contracting process, which includes proposal, review, and acceptance by both parties. Equinix has documented policies and procedures in place to facilitate implementation of new customers. Within the policies and procedures, responsibilities for each of the technical areas and standard service level definitions are delineated. Contracts executed for customers are specific and have varying service level definitions, according to the agreement(s) executed between Equinix and new customers. The Equinix legal team reviews each contract prior to approval. Items sold after contract signing, are transformed into work orders for commercial and thus automatically routed to the activation team.

Operations system (OS) work orders are documented in ServiceNow defining the internal services, infrastructure services or purchase of resources needed for the new customer implementation project. The management team, analyst, activation coordinator or manager perform a technical analysis of the new implementation project verifying that the products and services are within Equinix's product and company specifications. A technical interview is performed confirming the scope of the project with the customer who has up to 48 hours (2 days) to approve the project scope. After the project scope is confirmed by the customer, the technical analysis is approved, and the project is activated. Once the management team assigns the projects start and end date, a Welcome kit and detailed project plan is e-mailed to the customer. Technical interview documents are documented within ServiceNow throughout the project's entire life cycle.

Changes to Customer Assets

Control Objective: Control activities provide reasonable assurance that changes to customers' assets are authorized, tested and approved.

Equinix has documented change control policies and procedures to guide personnel in change management practices regarding the changes to existing customer assets and infrastructure software and hardware to ensure that changes are authorized, tested and approved before being implemented in the production environment.

Changes to customer assets typically include changes to communications, configurations, or installation of new devices, which can be initiated internally or by a customer request. When a customer asset change is identified, or a change is requested from a customer, helpdesk personnel document the details within a change request form, to track the changes throughout the change process to ensure that the change control procedures are followed. The change requestor is responsible for populating key fields within a request form, including the impact of the change, change type, brief description, test results, and approvals.

Helpdesk personnel are required to obtain customer authorization for changes to customer assets either by confirming the authorized customer via phone or required written documentation be provided via an e-mail. Change personnel are responsible for ensuring that functional testing is completed for changes prior to implementation into the production environment. Following successful testing, change personnel will obtain verification from testing personnel and update the test results on the change request form to denote that testing has been performed. A change management committee analyzes and approves change request forms by assessing the risks, impacts and back out plans prior to the change implementation.

Backup Management

Control Objective: Control activities provide reasonable assurance that the customers' data and business information is appropriately backed up.

Equinix has documented policies and procedures to communicate backup processes to relevant personnel to ensure systems are backed up in a timely manner and are securely stored. Backup systems are utilized to automate the backup process. These systems are configured to perform daily incremental backups, weekly and monthly full backups of production systems. Data backups are performed on daily, weekly and monthly basis based upon each customer specific requirements.

Operations personnel are responsible for managing the customer shared backup environment. Daily activities include the following:

- Monitor the progress of backup jobs;
- Monitor the availability of infrastructure;
- Guide the NOC in cases of treatment most basic backup errors;
- Treat backup errors;
- Interface with the suppliers for the cases of more advanced backup errors; and
- Advise and support new activations via the self-service portal.

Additionally, operations personnel are responsible for the following:

- Management of hardware and software resources;
- License management;
- Ensuring the availability of the environment;
- Ensuring environmental recovery in case of disaster;
- Monitoring indicators of executions; and
- Management of term support contracts with suppliers.

Operations personnel monitor the success and failure of data backups and are notified of the status of backup job completion via e-mail notifications. Operations personnel then investigate the causes of failures in order to identify if corrective actions need to be taken.

Backup media is stored on-site within secured rooms located within the data center facilities. Operations personnel perform backup restoration tests of backup media on a monthly basis for certain customers to ensure that the media can be restored completely and accurately. Additional data backup restorations are performed when requested by customers.

Issues and Incident Management

Control Objective: Control activities provide reasonable assurance that issues and incidents involving infrastructure and applications are identified, monitored, investigated and resolved in a timely manner.

Incident response and escalation policies and procedures are documented to efficiently and effectively manage incidents impacting the customer infrastructure and applications. A ticketing system is in place in order to document, escalate, and resolve system incidents. When an incident is detected, helpdesk personnel will examine the incident, review the incident alert and document the details in the ticketing system and attempt to troubleshoot the incident. If helpdesk personnel cannot resolve the incident, the ticket is escalated to get the necessary individuals involved to resolve the incident. Status updates related to the incident are logged in the ticketing system.

Issues and incidents can be initiated via client web portal access or via phone calls and directly by helpdesk support personnel. Equinix helpdesk personnel prioritize, and handle customer inquiries and infrastructure issues to ensure that problems identified are responded to in a timely manner. Helpdesk personnel actively monitor the enterprise tools on a 24 hour per day basis to help ensure the systems are available and operating properly. In the event that

a pre-defined severity level is exceeded, an on-screen incident alert is generated, and helpdesk personnel are required to investigate the issue/incident.

Network and System Monitoring

Control Objective: Control activities provide reasonable assurance that infrastructure and systems are monitored and problems are tracked, escalated and resolved in a timely manner.

Equinix has implemented network and system administration policies and procedures to help guide NOC personnel in the monitoring, prioritization, and handling of infrastructure issues to ensure that problems identified are investigated and resolved in a timely manner. Enterprise monitoring tools are utilized to monitor the health and availability of the overall production environment. The enterprise monitoring tools are in place on the production servers and infrastructure network to monitor for metrics that include the following:

- Zabbix (Central Processing Unit (CPU), memory, disk, availability)
- Wanguard (Intrusion Detection System (IDS))

Management utilizes IDS to monitor the production servers for potential or actual security breaches. The IDS is configured to log pre-defined events, including events originating from the same IP address, events with the same source and destination Internet protocol (IP) address, and events with the same source to multiple destination IP addresses, and repetitive attempts within a certain amount of time. NOC personnel are notified real time via automated e-mails in the event that predefined conditions are triggered. Additionally, NOC personnel review the logs periodically to investigate suspicious activity. In the event that a potential or actual security breach is encountered, NOC personnel work to remediate the breach immediately, and then work to determine the cause of the breach. Once the breach is resolved, NOC personnel log the resolution and remediation activities in a ticket.

Information Security Management

Control Objective: Controls provide reasonable assurance that the business needs, risk management, physical security, and information security culture are an integral part of a general plan for information security.

Equinix has policies and procedures in place to address aspects of information security that affect the delivery of services to customers. These policies include internet access, physical access, information classification, backup, data retention, and information security. Integrity and ethical values are essential elements of Equinix's control environment, affecting the design, administration, and monitoring of other components.

Requirements of employees are also communicated via documented position descriptions which define the skills, responsibilities, and knowledge levels required for particular jobs. Equinix's values and behavioral standards, including information security, are communicated to employees via the internal Equinix portal. Equinix personnel acknowledge that they have read and accept Equinix information security policies by achieving a passing score on the information security policy-based test. Management ensures information security objectives are consistent with customer, regulatory, and legal requirements by performing a review of information security objectives on an annual basis. Management meetings are performed to review and monitor compliance and corrective action initiatives on a quarterly basis.

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 Americas Data Center Hosting Services and Brasil Managed Services system. Equinix's internal systems supporting the Americas Data Center Hosting Services and Brasil Managed Services include Dell Blade servers running on Windows and Red Hat Enterprise Linux operating systems.

These internal systems are used to:

- Maintain customer information, work requests, and work history for the data center sites
- Design and dispatch orders to site operations and maintain information regarding utilized site assets
- Monitor customer service infrastructure
- Schedule and track maintenance on site infrastructure
- Collect, dispatch, and track customer support requests
- Identify on-call engineering resources for incident response and support escalation
- Track and identify customer port assignments
- Manage customer order workflow within operations
- Design site infrastructure layout for customer solutions
- Manage site security access control
- Record and monitor CCTV in each site

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. 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 particular 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 change review meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming 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 through direct relationships with Equinix personnel. Examples of external communication methods are included below:

- Equinix's security and availability commitments and the associated system requirements are documented in customer agreements and via IBX product policies published to the company website.
- Changes, incidents, and outages related to security and availability at the data centers are communicated to customer and external users of the system via e-mail advisory notifications. If incidents are communicated through the online portal, personnel follow documented incident response plan. All incidents are processed according to Equinix global procedures following the Equinix global incident flowchart. All incidents are documented within the ticketing system and tracked by management until resolved.
- 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:

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

Monitoring of Subservice Organizations

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

Reporting 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 Americas Data Center Hosting Services and Brasil Managed Services system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to Equinix's Americas Data Center Hosting Services and Brasil Managed Services system to be solely achieved by Equinix's control activities. Accordingly,

user entities, in conjunction with the Americas Data Center Hosting Services and Brasil Managed Services, should establish their own internal controls or procedures to complement those of Equinix.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls that ensure notifying Equinix of changes made to technical or administrative contact information.	Physical Security
User entities are expected to implement controls that ensure providing and maintaining the facility access list of authorized personnel, vendors and contractors.	
User entities are expected to implement controls that ensure notifying Equinix of on-site visits of employees, vendors, and contractors prior to arrival at the data center.	
User entities are expected to implement controls that ensure adhering to the Equinix physical security and safety procedures.	
User entities are expected to implement controls that ensure informing their vendors of the Equinix security and safety procedures.	
User entities are expected to implement controls that ensure their guests /visitors are escorted, as appropriate, throughout the Equinix facility.	
User entities are expected to implement controls that ensure the security of any keys or badges and confidentiality of any combinations used to access Equinix’s facilities.	
User entities are expected to implement controls that ensure their cabinets are locked and their equipment is secured prior to leaving the premises.	
User entities are expected to implement controls that ensure immediately notifying Equinix of the loss of or damage to equipment.	
User entities are expected to implement controls that ensure their hardware, software, data, and other equipment is insured.	
User entities are expected to implement controls that ensure the development of policies and procedures to protect their systems from unauthorized or unintentional use, modification, addition or deletion.	
User entities are expected to implement controls that ensure their understanding and complying with their contractual obligations to Equinix.	
User entities are responsible for communicating to Equinix the authorization for changes to customer assets prior to implementation.	Changes to Customer Assets
User entities are responsible for immediately notifying Equinix of any actual or suspected information security breaches, including compromised user accounts.	Issues and Incident Management
User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Equinix’s systems.	Information Security Management

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Americas Data Center Hosting and Brasil Managed Services system provided by Equinix. The scope of the testing was restricted to the Americas Data Center Hosting and Brasil Managed Services system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period November 1, 2019, through October 31, 2020.

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 specified control objectives were achieved during the reporting 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.

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 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 at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the “Complementary Controls at User Entities” within Section 3. Control considerations that should be implemented by subservice organizations in order to complement the control activities and achieve the stated control objective are presented in the “Complementary Controls at Subservice Organizations” within Section 3.

PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that physical access to Equinix IBX locations, facility infrastructure platforms, and customer footprint(s) is limited to properly authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Corporate Support			
1.01	Documented physical security standard operating procedures (SOPs) approved by management exist to provide guidance on restricting and controlling access to the data center facilities.	Inspected the physical security policies and procedures to determine that documented physical security SOPs approved by management were in place to provide guidance on restricting and controlling access to the data center facilities.	No exceptions noted.
Data Center Facilities			
1.02	Procedures exist and are followed to establish and make changes to physical access privileges for employees.	Inquired of the data center managers regarding physical access procedures to the data center facilities to determine that procedures were in place and followed to establish and make changes to physical access privileges for employees.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access request tracking documentation for a sample of employees hired during the reporting period to determine that procedures existed and were followed to grant physical access privileges for each employee sampled.	No exceptions noted.
		Inspected the access termination tracking documentation for a sample of employees terminated during the reporting period to determine that procedures existed and were followed to revoke physical access privileges for each employee sampled.	No exceptions noted.
1.03	Procedures exist and are followed to established and make changes to physical access privileges for customers.	Inquired of the data center managers regarding physical access procedures to the data center facilities 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 change tracking documentation for a sample of customer physical access change requests received during the reporting period to determine that procedures were followed to establish and make changes to physical access privileges for customers to each facility.	No exceptions noted.
1.04	Security personnel review a government issued ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to the facility.	Observed the physical access procedures at the data center facilities to determine that security personnel reviewed a government issues ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.05	Visitor access procedures are in place requiring: <ul style="list-style-type: none"> • Visitor sign into a log upon entry to the facility • Visitors are to be escorted by an authorized employee when accessing the facilities 	Inquired of the data center managers regarding visitor access procedures to the data center facilities to determine that visitors were required to sign in and be escorted by an authorized employee when accessing the facilities.	No exceptions noted.
		Observed the physical access procedures at the data center facilities to determine that visitors were required sign in and be escorted by an authorized employee when accessing each facility.	No exceptions noted.
1.06	For North America facilities that employ onsite security, KPIs are reported and reviewed monthly to help ensure performance metrics are met and that security personnel completed required trainings.	Inquired of the IBX site managers regarding security personnel training procedures for the data center facilities to determine that for North America facilities that employed onsite security personnel, KPIs were reported and reviewed monthly to help ensure performance metrics are met and that security personnel completed required trainings.	No exceptions noted.
		Inspected the KPI and scorecard summary reports for a sample of North America data center facilities and months during the reporting period to determine that KPIs were reported and reviewed for each month and facility sampled.	No exceptions noted.
1.07	A proximity card system and / or a biometric reader and PIN are required to restrict access to the facility. Access to the colocation areas requires a valid badge access card.	Observed the physical access control systems in place at the data center facilities to determine that a proximity card system and / or a biometric reader and PIN were in place to restrict access to each facility.	No exceptions noted.
1.08	Physical access system logs are recorded and maintained for a minimum of six months.	Observed the historical physical access system logs maintained for the data center facilities to determine that physical access system logs were available for at least six months from the date of observation for each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the historical physical access control and visitor management systems logs maintained for a sample of data center facilities to determine that physical access system logs were recorded and retained for at least six months from the date of inspections for each facility.	No exceptions noted.
1.09	Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.	Observed the monitoring procedures at the data center facilities to determine that monitoring of physical activity was performed through the use of onsite security monitoring and/or digital surveillance cameras at each facility.	No exceptions noted.
		Inspected the security monitoring shift schedules for a sample of data center facilities and months during the reporting period to determine that onsite and offsite security personnel were scheduled 24x7 to monitor each facility during each month sampled.	The test of the control activity disclosed that the third-party security guard schedule was not available for one of 41 IBX data center facilities sampled for one of three months sampled.
1.10	CCTV surveillance cameras are in place to monitor and record activity at the entrances to and throughout the data center facilities. Surveillance camera logs are recorded and maintained for a minimum of 30 days.	Inquired of the data center managers regarding surveillance camera log retention procedures at the data center facilities to determine that CCTV surveillance cameras are in place to monitor and record activity at the entrances to and throughout the data center facilities and surveillance camera footage was recorded and maintained for a minimum of 30 days.	No exceptions noted.
		Observed the historical surveillance camera logs maintained for the data center facilities to determine that surveillance camera footage was available for review at least 30 days from the date of observation for each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the historical surveillance camera logs for a sample of data center facilities to determine that surveillance camera footage was available for review at least 30 days from the date of observation for each facility sampled.	No exceptions noted.
1.11	Access to the colocation areas requires a valid badge access card. Each customer has a defined space within the data center that is physically secured within a locked cage and / or cabinet.	Observed an example employee attempt to access colocation areas at data center facilities to determine that access to the colocation areas required a valid badge access card for each facility.	No exceptions noted.
		Observed the colocation space at the data center facilities to determine that customers had defined space within the data center that were physically secured within a locked cage and / or cabinet for each facility.	No exceptions noted.
1.12	Customers are required to sign a contract 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 reporting period to determine that a stating Equinix's security and availability commitments, the associated system requirements and a nondisclosure agreement was in place for each customer sampled.	No exceptions noted.
1.13	The data center floor does not have any windows leading to the exterior of the building. In case due to the existing infrastructure there are windows leading to the exterior then they need to be locked from the inside or access controlled.	Observed the colocation space at data center facilities to determine that the data center floor did not have any windows leading to the exterior of the building or in the case due to the existing infrastructure there were windows leading to the exterior, those windows were locked from the inside or access controlled for each facility	No exceptions noted.
1.14	Colocation area exterior walls extend from the floor to the ceiling.	Observed the colocation area exterior walls at the data center facilities to determine that colocation area exterior walls extended from the floor to the ceiling for each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.15	Physical access reviews for data center facilities in South America are documented and approved on a quarterly basis by information security personnel.	Inspected the physical access review policy and the access reviews for a sample of South America data center facilities and quarters during the reporting period to determine that physical access reviews for each data center facility sampled were documented and approved by information security personnel for each quarter sampled.	The test of the control activity, performed in August 2020, disclosed that a physical access review was not performed for one of two quarters sampled, for six of six data center facilities sampled. Additional testing of the control activity, performed in September 2020, disclosed that a physical access review was performed for two of three quarters sampled, for the aforementioned data center facilities.

ENVIRONMENTAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that Equinix facilities housing customer equipment and support operations are engineered and monitored to reduce the risk of environmental threats (i.e., power loss, fire, and flooding).

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Corporate Support			
2.01	Documented environmental security SOPs have been approved by management and are in place to help ensure that facilities have a consistent level of facility and environmental protection.	Inspected the environmental security SOPs to determine that environmental security SOPs were approved by management and included guidance regarding facility environmental protection.	No exceptions noted.
Data Center Facilities			
2.02	Each facility has been inspected by a local government official to ensure building code requirements have been met.	Inquired of the data center managers regarding the building code requirements to determine that each data center facility had been inspected by a local government official to ensure building code requirements had been met.	No exceptions noted.
		Inspected the certificate of occupancy for a sample of data center facilities to determine that a certificate of occupancy was in place evidencing inspection by a local government official for each facility sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.03	Each facility is monitored 24x7 by onsite or on call facilities engineers.	Observed the facility monitoring procedures at the data center facilities to determine that each facility was monitored by facilities engineers during standard business hours.	No exceptions noted.
		Inspected the data center facility engineer staffing schedules for a sample of data center facilities and months during the reporting period to determine that onsite or on call facilities engineers were scheduled 24x7 to monitor each facility during each month sampled.	No exceptions noted.
2.04	A BMS is used to monitor the critical facility equipment and alert personnel of any potential issue.	Observed the BMS at the data center facilities to determine that a BMS was in place to monitor the critical facility equipment and alert personnel when potential issues were identified for each facility.	No exceptions noted.
		Inspected the BMS monitoring dashboard and example alert log notifications generated during the reporting period for a sample of data center facilities to determine that a BMS was used to monitor the critical facility equipment and alert personnel when potential issues were identified for each facility sampled.	No exceptions noted.
2.05	Power management equipment is in place for each facility.	Observed the power management equipment at the data center facilities to determine that power management equipment was in place at each facility.	No exceptions noted.
2.06	Scheduled maintenance procedures are performed to test and confirm the operation of the power management systems.	Observed the power management system maintenance documentation onsite with the assistance of facilities personnel at the data center facilities to determine that scheduled maintenance procedures were performed to test and confirm the operation of the power management systems during the reporting period at each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent UPS and generator preventative maintenance reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed for the power management systems during the reporting period for each facility sampled.	No exceptions noted.
2.07	Fire detection and suppression equipment is in place at each facility.	Observed the fire detection and suppression equipment at the data center facilities to determine that fire detection and suppression equipment was in place at each facility.	No exceptions noted.
2.08	Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.	Observed the fire extinguisher maintenance documentation onsite with the assistance of facilities personnel at the data center facilities to determine that scheduled maintenance procedures were performed to help ensure that fire extinguishers were working properly during the reporting period at each facility.	No exceptions noted.
		Inspected the most recent fire detection and suppression equipment preventative maintenance reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed for the fire detection and suppression equipment during the reporting period for each facility sampled.	No exceptions noted.
2.09	Air conditioning and ventilation equipment is in place at each facility to ensure that humidity levels and the required temperature are maintained.	Inquired of the data center managers regarding the HVAC equipment at the data center facilities to determine that HVAC equipment was in place to ensure that humidity levels and the required temperature were maintained at each facility.	No exceptions noted.
		Observed the HVAC equipment at the data center facilities to determine that air conditioning and ventilation equipment was in place at each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.10	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 data center facilities to determine that scheduled maintenance procedures were performed for the HVAC equipment during the reporting period for each IBX facility sampled.	No exceptions noted.
2.11	Insurance is in place for the data center locations and equipment.	Inspected the certificate of property insurance for the data center facilities to determine that the data center locations and equipment were covered under an active insurance policy during the reporting period.	No exceptions noted.
2.12	Leak detection equipment is in place to help detect water presence where there should be none.	Observed the leak detection equipment at the data center facilities to determine that leak detection equipment was in place near water sources to help detect water presence, where there should be none, at each facility.	No exceptions noted.
2.13	Production equipment within the data center facilities are placed on racks to protect infrastructure from localized flooding.	Observed the server racks at the data center facilities to determine that production equipment within the data center facilities were placed on racks to protect infrastructure from localized flooding.	No exceptions noted.
2.14	Emergency procedure documentation approved by management that addresses fires, bomb threats, severe weather, and medical emergencies is in place.	Inspected the IBX emergency policies and procedures and the security staff procedures to determine that management approved emergency procedures were in place that addressed fires, bomb threats, severe weather, and medical emergencies.	No exceptions noted.

NEW CUSTOMER IMPLEMENTATION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new customers are implemented in line with contractual requirements.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.01	Documented policies and procedures are in place for the implementation of new customers.	Inspected the policies and procedures for the implementation of new customers to determine that documented policies and procedures were in place for the implementation of new customers.	No exceptions noted.
3.02	Service level agreements are formally documented and approved prior to new customer implementations.	Inspected the service level agreements for a sample of new customers implemented during the reporting period to determine that service level agreements were formally documented and approved prior to new customer implementations for each new customer implementation sampled.	No exceptions noted.
3.03	Work orders are submitted upon contract signature to implement services according to product specifications.	Inquired of the security and compliance manager regarding work orders to determine that work orders were submitted upon contract signature to implement services according to product specifications.	No exceptions noted.
		Inspected work orders for a sample of new customers implemented during the reporting period to determine that work orders were submitted upon contract signature to implement services according to product specifications for each new customer implementation sampled.	No exceptions noted.
3.04	Technical interviews are completed and documented within the ticketing system detailing the scope of the implementation.	Inquired of the security and compliance manager regarding technical reviews to determine that technical interviews were completed and documented within the ticketing system detailing the scope of the implementation.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the technical interview documents for a sample of new customers implemented during the reporting period to determine that technical interviews were completed and documented within the ticketing system detailing the scope of the implementation for each new customer implementation sampled.	No exceptions noted.
3.05	Customers approve implementation services prior to activation.	Inspected the approvals for a sample of new customers implemented during the reporting period to determine that customers approved implementation services prior to activation for each new customer implementation sampled.	No exceptions noted.

CHANGES TO CUSTOMER ASSETS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to customers' assets are authorized, tested and approved.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.01	Documented change control policies and procedures are in place to guide personnel in change management practices including, but not limited to, the following: <ul style="list-style-type: none"> • Change request • Approval process • Review process • Testing of changes 	Inspected policy documentation to determine that documented change control policies and procedures were in place that included the following: <ul style="list-style-type: none"> • Change request • Approval process • Review process • Testing of changes 	No exceptions noted.
4.02	Change management department personnel utilize a helpdesk ticketing system to track, monitor, and report the status of each change ticket.	Inspected the helpdesk ticketing system to determine that change management department personnel utilized a helpdesk ticketing system to track, monitor, and report the status of each change ticket.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.03	Management utilizes a standard change request form to document changes to customer assets.	Inspected the change request forms for a sample of changes implemented during the reporting period to determine that a standard change request form was utilized for each change sampled.	No exceptions noted.
4.04	Helpdesk personnel are required to obtain customer authorization for changes to customer assets prior to implementation.	Inquired of the security and compliance manager regarding helpdesk requirements to determine that helpdesk personnel were required to obtain customer authorizations for changes to customer assets prior to implementation.	No exceptions noted.
		Inspected the change request forms for a sample of changes implemented during the reporting period to determine that helpdesk personnel obtained customer authorizations prior to implementation for each change sampled.	No exceptions noted.
4.05	Change personnel perform functional testing for changes to customer assets prior to implementation.	Inspected change request forms for a sample of changes implemented during the reporting period to determine that change personnel performed functional testing prior to implementation for each change sampled.	No exceptions noted.
4.06	The change management committee approves changes to customer assets prior to implementation.	Inspected the change approval documentation for a sample of changes implemented during the reporting period to determine that the change management committee approved changes to customer assets prior to implementation for each change sampled.	No exceptions noted.

BACKUP MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the customers' data and business information is appropriately backed up.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.01	Documented backup policies and procedures are in place to guide operations personnel in the backup and storage of production data and systems.	Inspected the policy and procedure documentation to determine that documented data backup policies and procedures were in place and addressed the backup and storage of production data and systems.	No exceptions noted.
5.02	Management utilizes an automated backup system to perform scheduled backups of production systems.	Inquired of the data backup team leaders regarding the automated backup system to determine that management utilized an automated backup system to perform scheduled backups of production systems.	No exceptions noted.
		Inspected the automated backup system configurations and software versions to determine that management utilized an automated backup system to perform scheduled backups of production systems.	No exceptions noted.
5.03	The automated backup system is configured to perform incremental backups of production systems on a daily basis and full backups on a weekly basis.	Inspected the automated backup system configurations for a sample of customers and example backup summary logs generated during the reporting period to determine that the automated backup system was configured to perform incremental backups of production systems on a daily basis and full backups on a weekly basis for each customer sampled.	No exceptions noted.
5.04	The automated backup systems are configured to notify systems administration personnel via e-mail regarding the status of backup job completion.	Inspected the notification configurations for the automated backup systems and an example e-mail notification generated during the reporting period to determine that the automated backup systems were configured to notify systems administration personnel via e-mail regarding the status of backup job completion.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.05	Operations personnel perform restoration of backup data on a monthly basis and upon customer request and document job details in monthly reports.	Inquired of the data backup team leaders regarding data restorations to determine that operations personnel performed restoration of backup data on a monthly basis and upon customer request and documented job details in monthly reports.	No exceptions noted.
		Inspected the data backup restore reports for a sample of months performed during the reporting period to determine that operations personnel performed restoration of backup data on a monthly basis and upon customer request and documented job details in monthly reports for each month sampled.	No exceptions noted.
5.06	Management maintains on-site backup media within secured areas located within the data center facilities.	Observed the storage of on-site backup media at the data center facilities to determine that management maintained on-site backup media within secured areas located within the data center facilities.	No exceptions noted.

ISSUES AND INCIDENT MANAGEMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that issues and incidents involving infrastructure and applications are identified, monitored, investigated and resolved in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.01	Documented issue and incident policies and procedures are in place to guide personnel in issue and incident practices that include, but are not limited to, the following: <ul style="list-style-type: none"> • Infrastructure • Network • Application 	Inspected the issue and incident policies and procedures to determine that documented issue and incident policies and procedures were in place that included the following: <ul style="list-style-type: none"> • Infrastructure • Network • Application 	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.02	Helpdesk support personnel utilize a helpdesk ticketing system to identify, manage and track issues and incidents for response and resolution.	Inquired of the assistant project and program manager regarding the helpdesk ticketing system to determine that helpdesk support personnel utilized a helpdesk ticketing system to identify, manage and track customer inquiries and issues for response and resolution.	No exceptions noted.
		Inspected the helpdesk ticketing system and a sample of tickets generated during the reporting period to determine that a helpdesk ticketing system was utilized to manage and track issues and incidents for response and resolution.	No exceptions noted.

NETWORK AND SYSTEM MONITORING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that infrastructure and systems are monitored and problems are tracked, escalated and resolved in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.01	<p>Documented network and systems monitoring policies and procedures are in place to help guide NOC personnel in monitoring, prioritization, and handling of customer inquiries and issues that include, but are not limited to, the following:</p> <ul style="list-style-type: none"> Enterprise monitoring application procedures Alarm and alert processes Outage notification handling 	<p>Inspected the policy and procedure documentation to determine that management documented network and systems monitoring policies and procedures were in place to help guide NOC personnel in monitoring, prioritization, and handling of customer inquiries and issues that included the following:</p> <ul style="list-style-type: none"> Enterprise monitoring application procedures Alarm and alert processes Outage notification handling 	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.02	Enterprise monitoring applications are utilized to monitor the performance and availability of production servers and network infrastructure.	Inspected the configurations for the enterprise monitoring applications to determine that enterprise monitoring applications were utilized to monitor the performance and availability of production servers and network infrastructure.	No exceptions noted.
7.03	NOC personnel are available to monitor and address system alerts generated from the monitoring applications 24 hours per day.	Inquired of the assistant project and program manager regarding the monitoring activities of the NOC personnel to determine that NOC personnel were available to monitor and address system alerts generated from the monitoring applications 24 hours per day.	No exceptions noted.
		Inspected the NOC personnel schedule for a sample of months during the reporting period to determine that NOC personnel were scheduled 24 hours per day for each month sampled.	No exceptions noted.
7.04	An IDS is utilized to analyze network events for possible or actual network security breaches.	Inspected the IDS dashboard and an example IDS log generated during the reporting period to determine that an IDS was utilized to analyze network events for possible or actual network security breaches.	No exceptions noted.
7.05	NOC personnel monitor the IDS system on a real-time basis to analyze network events for possible or actual network security breaches.	Inquired of the security and compliance manager regarding the IDS system to determine that NOC personnel monitored the IDS system on a real-time basis to analyze network events for possible or actual network security breaches.	No exceptions noted.
		Inspected the NOC personnel monthly schedule for a sample of months during the reporting period and IDS alert configurations to determine that NOC personnel monitored the IDS system on a real-time basis to analyze network events for possible or actual network security breaches.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.06	A ticketing system is in place to document, escalate, and resolve system availability issues.	Inspected the ticketing system console and a sample of incident tickets closed during the reporting period to determine that a ticketing system was in place to document, escalate, and resolve system availability issues.	No exceptions noted.
7.07	NOC management personnel meetings are held on a monthly basis to review and resolve any monitoring issues noted.	Inspected the monthly meeting presentation for a sample of months during the reporting period to determine that NOC management personnel meetings were held for each month sampled to review and resolve monitoring issues noted.	No exceptions noted.

INFORMATION SECURITY MANAGEMENT

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that the business needs, risk management, physical security, and information security culture are an integral part of a general plan for information security.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.01	<p>Documented information security policies and procedures are in place to guide personnel in security practices that include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • Internet access • Physical access • Backup • Information classification • Data retention • Information security 	<p>Inspected policy and procedure documentation to determine that documented information security policies and procedures were in place to guide personnel in performing information security practices that included the following:</p> <ul style="list-style-type: none"> • Internet access • Physical access • Backup • Information classification • Data retention • Information security 	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.02	Management communicates information security policy and procedure changes and relevant updates to employees via the internal intranet.	Inspected a screen print of the Equinix intranet site to determine that management communicated information security policy and procedure changes and relevant updates to employees via the internal intranet.	No exceptions noted.
8.03	Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the company organizational charts to determine that organizational charts were in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
8.04	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented position descriptions for a sample of active employment positions to determine that documented position descriptions were in place for each employment position sampled to define the skills and knowledge levels required for the competence levels of particular jobs.	No exceptions noted.
8.05	Employees are required to sign an acknowledgment form indicating that they have been given access to the information security policies and understand their responsibility for adhering to the policies and procedures contained within the policy.	Inspected the acknowledgment form for a sample of employees hired during the reporting period to determine that each employee sampled signed an acknowledgment form indicating that they had been given access to the information security policies and understood their responsibility for adhering to the policies and procedures contained within the policy.	No exceptions noted.
8.06	Information security personnel perform a review of information security objectives on an annual basis.	Inquired with the security and compliance manager regarding the information security review to determine that information security personnel performed a review of internal information security objectives on an annual basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent information security review to determine that information security personnel performed a review of internal information security objectives during the reporting period.	No exceptions noted.
8.07	Administrator access within the badge access system is restricted to user accounts accessible by authorized personnel.	Inspected the screen prints of users with administrative privileges to the badge access system to determine that administrator access privileges within the badge access system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
8.08	Management meetings are held to review and monitor compliance and corrective action initiatives on a quarterly basis.	Inquired of the security and compliance manager regarding the management meetings to determine that management meetings were held to review and monitor compliance and corrective action initiatives on a quarterly basis.	No exceptions noted.
		Inspected the information security committee meetings for a sample of quarters during the reporting period to determine that management meetings were held to review and monitor compliance and corrective action initiatives for each quarter sampled.	The test of the control activity disclosed that information security committee meetings were not held for one of two quarters sampled.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Physical Security

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.09	Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.	Inspected the security monitoring shift schedules for a sample of data center facilities and months during the reporting period to determine that onsite and offsite security personnel were scheduled 24x7 to monitor each facility during each month sampled.	The test of the control activity disclosed that the third-party security guard schedule was not available for one of 41 IBX data center facilities sampled for one of three months sampled.
Management's Response:	Management will review with site security and third-party security to reinforce process and make sure schedules will be available.		

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.15	Physical access reviews for data center facilities in South America are documented and approved on a quarterly basis by information security personnel.	Inspected the physical access review policy and the access reviews for a sample of South America data center facilities and quarters during the reporting period to determine that physical access reviews for each data center facility sampled were documented and approved by information security personnel for each quarter sampled.	The test of the control activity, performed in August 2020, disclosed that a physical access review was not performed for one of two quarters sampled, for six of six data center facilities sampled. Additional testing of the control activity, performed in September 2020, disclosed that a physical access review was performed for two of three quarters sampled, for the aforementioned data center facilities.
Management's Response:	Management will review with site security and site staff and will continually monitor for compliance.		

Information Security Management

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.08	Management meetings are held to review and monitor compliance and corrective action initiatives on a quarterly basis.	Inspected the information security committee meetings for a sample of quarters during the reporting period to determine that management meetings were held to review and monitor compliance and corrective action initiatives for each quarter sampled.	The test of the control activity disclosed that information security committee meetings were not held for one of two quarters sampled.
Management's Response:	Management will review its information security committee meetings process.		