EQUINIX

SOC 1 REPORT

FOR

DATA CENTER HOSTING 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

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.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Equinix, Inc.:

Scope

We have examined Equinix, Inc.'s ("Equinix" or "service organization") description of its Data Center Hosting Services system performed in Germany, United Kingdom, France, The Netherlands, Switzerland, Ireland, Sweden, Finland, United Arab Emirates, Spain, Portugal, Turkey, Bulgaria, Italy, and Poland 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 Data Center Hosting 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.

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 Data Center Hosting 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 Data Center Hosting 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 Data Center Hosting 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 Data Center Hosting 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 Data Center Hosting 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 Data Center Hosting 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.

Scheelman & Company, LLC

Tampa, Florida
November 24, 2020

Section 2

Management's Assertion

MANAGEMENT'S ASSERTION

We have prepared the description of Equinix, Inc.'s ("Equinix") Data Center Hosting Services system performed in Germany, United Kingdom, France, The Netherlands, Switzerland, Ireland, Sweden, Finland, United Arab Emirates, Spain, Portugal, Turkey, Bulgaria, Italy, and Poland 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.

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 Data Center Hosting 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 Data Center Hosting Services system during the period covered by the description; and

iii. does not omit or distort information relevant to the scope of the Data Center Hosting 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 Data Center Hosting 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 54 markets on five continents and hosts a comprehensive portfolio of digital services and ecosystems that allows customers to securely scale their digital infrastructure wherever opportunity leads. More than 9,800 companies populate Equinix's diverse ecosystems, and all are potential partners or customers.

Description of Services Provided

Colocation Services

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

Physical Security

IBX Infrastructure

Each IBX data center utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. Exterior walls may incorporate additional security measures, such as reinforced concrete, electric fencing, Kevlar bullet board, vapor barriers, or bullet-resistant front doors. Colocation and IBX floor areas have window-less exteriors. In 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 industry rated ballistic protection.

All areas of the data center, including cages, are monitored, and recorded using closed circuit television (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. The alarm monitoring/intrusion detection subsystem monitors the status of various devices associated with the security system, such as alarm contacts, glass breakage detectors, motion detectors, and tamper switches. If the status of any of these devices changes from their secure state, an alarm will be activated and displayed on the security system workstation and recorded on the system server's hard drive.

The IBX data centers are staffed and/or monitored on a 24-hour basis by professional security staff, which monitors access points and monitors the electronic security systems. At each IBX, where there is a minimum of two security officers, at least one officer needs to be present to man the security kiosk and any additional officers may perform rounds of the IBX. Doors, including cages are secured with biometric hand geometry readers or proximity card readers. Each cage door has an auto lock mechanism that triggers 4 to 5 seconds of the door being unlocked. For shared cages, there are locks on the cabinets. Security systems have dedicated uninterruptible power supply (UPS) systems and standby emergency power (generator) support.

Other security features and controls may include:

- Control points between exterior and customer equipment
- 90-day video activity storage (subject to local country law)
- Weekly cross-IBX security meetings
- Customer self-administration of authority levels for ordering and access
- Segregation of order management (done by customer service and/or sales) and service delivery IBX functions in order to assure no local agreements

- Customer privacy policies, including no pictures and customer anonymity
- Facility design, which includes controlled access points, reinforced exterior walls
- Token authentication required for access to enterprise network
- Bullet-resistant protection
- Motion-detection lighting

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

Equinix uses biometric hand scanners to allow authorized users access into the building and through various doors within the facility. Through a combination of hand scan and numeric code, users identify themselves to the system and obtain access into certain areas of the IBX based upon the predefined user permissions. Biometric scanners are not required on the colocation side of doors to exit the colocation area into the customer care / common areas. Entry to customer cages from the exterior to the IBX requires access from a minimum of three to four access controls. Cage security is provided through multiple levels of access control: hand geometry readers at the cage entrance (subject to customer requirement), keyed locks at each cage or access card reader at each cage, and if the cabinet is located in a shared-cage environment, the cabinet door includes a lock. Access histories can be downloaded by Equinix personnel and are available to the customer for auditing purposes through SmartHands. 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.

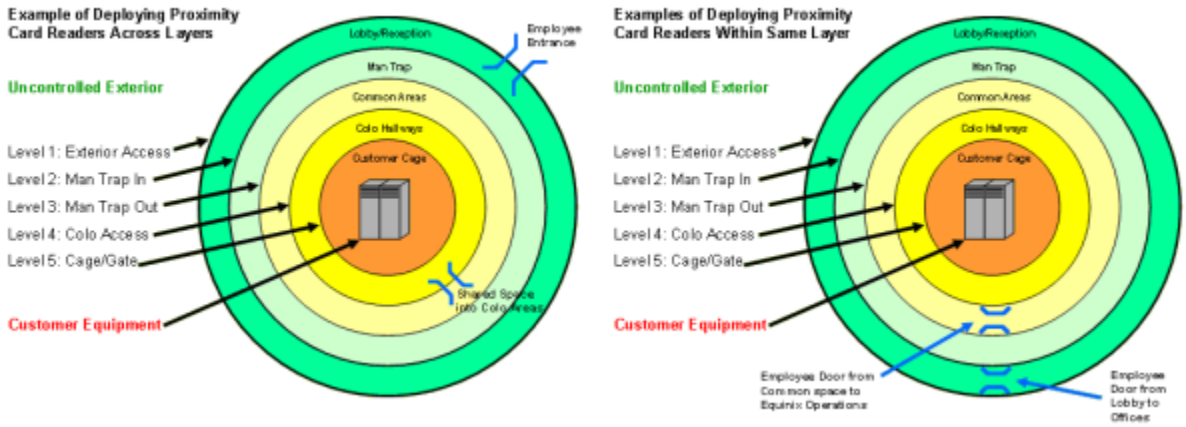
Employee Data Center Access

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. It is Equinix company policy to issue identification badges to each Equinix employee and to a temporary agency. These policies apply to employees, trainees, temporary agency workers. Equinix EMEA IBXs maintain a role-based employee access list. Access is immediately revoked once an employee is terminated or leaves the organization. Changes to employee roles and transfers also trigger an update to the Employee Secure Access List.

Personnel authorized to work at an Equinix facility are required to display identification badges when entering or working within an Equinix IBX. For employees, a service request (SR) or an e-mail notification needs to be opened in order for a hand scan to be approved. Depending on the access privileges, off-site employees may be required to be escorted by authorized personnel while within the facility. Offsite employees are screened upon entry to verify their identity. The security guard checks the government issued photo identification and visitors are required to sign in.

Equinix employees are given a proximity access card as per their role in the IBX. Equinix has a defined policy for the same as per role. These proximity access cards are to be returned back to security every time the employee leaves the premises.

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. Intercom radios with cameras are installed at vehicle access gates at IBX locations, which control access to areas surrounding shipping / receiving doors and/or loading docks.



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

Customer Data Center Access

Customers are required to sign a contract and a nondisclosure agreement with Equinix. Customers, customer contractors and customer visitors are screened upon entry to verify their identity. The security guard checks the government issued photo identification and visitors are required to sign in. Authorized customers are provided a unique identifier and password and granted access via specific roles within the Equinix Customer Portal (ECP). ECP is the primary database for Equinix's customer contacts.

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

Vendor and Contractor Data Center Access

Vendors and contractors follow access procedures similar to those of customers. Vendors and contractors are screened upon entry to verify their identity. The security guard checks the government issued photo identification and visitors are required to sign in. For an Equinix contractor, 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 personnel or security.

Visitor Data Center Access

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

Physical Access Removal

Biometric reader access to the IBX-secured areas is removed upon receipt of customer request by security. Access enrollment account removals are a priority status and must be acted upon within two hours of receiving the notification in Siebel. In order to help ensure tracking and customer notification, access enrollment removal requires a Siebel work ticket (SR) that is converted to a Siebel Security Console ticket. The security officer records the SR completion in Siebel Security Console.

After the access enrollment rights have been removed, access cards associated with the user are also canceled. In order to maintain accurate history records, individuals are never deleted from an access list. They are moved from an active to an inactive status.

Security Personnel Formal Training

All security officers are required to complete mandatory security training prior to their full-time assignment at Equinix. Security personnel formal training includes security-specific training that the security service provider provides its officers and Equinix specific training once they are assigned to Equinix. A summary of the training includes the following:

- Equinix company overview
- Safety training videos and/or classes
- Walkthrough of the IBX and orientation of the various equipment
- 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 record is maintained of the completed training and trainee sign acknowledging the completion of the training. In addition to the training, the trainee is continuously monitored by the senior security officer on-site until he/she is comfortable and confident carrying out all the assigned responsibilities.

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

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

Facility and Environmental Protection

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

The overriding criteria in the build of Equinix IBX facilities are that critical mechanical and electrical components are designed with adequate redundancy. 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 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 health and safety program and a headquarters-based H&S representative. This health and safety representative functions as an advisor 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 Building Management System (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 and pager.

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 heating, ventilation, and air-conditioning (HVAC) system, which controls and/or monitors space temperature and humidity within the IBX facilities, space pressurization, HVAC equipment status and performance, and outside air conditions
- Fire detection and suppression equipment, such as very early smoke detection apparatus (VESDA), double interlock pre-action and detection systems, and zoned gaseous-based fire extinguishing system
- Leak detection systems

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

Fire Detection and Suppression

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

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

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

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

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

Power Management Utility and Backup Power

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

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

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

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

Each IBX facility is built with zoned temperature control systems. Equinix maintains multiple air handling units at each IBX facility to verify correct temperature and humidity in critical areas. The air handling units in conjunction with a central HVAC plant work to maintain temperature and humidity levels. The average temperature of the supply

air to each zone is maintained between 64.4 degrees and 80.6 degrees Fahrenheit (or between 18 degrees and 27 degrees Celsius). If the temperature or humidity varies outside preset limits, an alarm is generated, and facilities personnel are notified. In some cases, to meet customer needs in high-density equipment areas, the supply air temperature to a region may be lower than 64.4 degrees Fahrenheit (18 degrees Celsius).

Leak Detection System

A leak detection system is installed, surrounding the "at-risk" areas within the building that monitors for water. Each IBX facility 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 Technical Facilities Manager (TFM) or a site engineer makes regular scheduled rounds. The rounds made are staggered to help ensure maximum equipment coverage.

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

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

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

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

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

Boundaries of the System

The scope of the review includes the Data Center Hosting Services performed at the data center facilities located in the metropolitan areas listed below. The specific control objectives and related control activities included within the scope of this engagement can be found in Section 4 of this document.

[Intentionally Blank]

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

#	Region	Site	Location
1	UK	LD3	Unit 11 Matrix, Coronation Road, Park Royal, London NW10 7PH
2		LD4	2 Buckingham Avenue, Slough Trading Estate, Slough, Berkshire SL1 4NB
3		LD5	8 Buckingham Avenue, Slough Trading Estate, Slough, Berkshire SL1 4AX
4		LD6	352 Buckingham Avenue, Slough Trading Estate, Slough, Berkshire SL1 4PF
5		LD7	1 Banbury Avenue, Slough, SL1 4LH
6		LD8	6/7/8/9 Harbour Exchange Square London E14 9GE
7		LD9	Unit 2 Powergate Business Park Volt Avenue, London NW10 6PW
8		LD10	13 Liverpool Road Slough, SL1 4QZ
9		LD13x	13 Liverpool Road Slough, SL1 4QZ
10		MA1	Unit 3 Williams House Manchester Science Park Lloyd Street N Manchester M15 6SE
11		MA2	Reynolds House Manchester Technopark Archway, Manchester M15 5RN
12		MA3	Joule House 76 Trafford Wharf Road Trafford Park, Manchester M17 1HE
13		MA4	Unit 4 Synergy House Manchester Science Park, Guildhall Close Manchester M15 6SY
14	Ireland	DB1	Unit 4027 Kingswood Road Citywest Business Campus Dublin 24
15		DB2	Unit 7, Kilcarbery Park New Nangor Road Dublin, 22
16		DB3	Unit 2 Northwest Business Park Ballycoolin Dublin 15
17		DB4	Unit 14 Northwest Business Park Ballycoolin Dublin 15
18	The Netherlands	AM1	Luttenbergweg 4, 1101 EC Amsterdam
19		AM2	Luttenbergweg 4, 1101 EC Amsterdam
20		AM3	Science Park 610, 1098 XH Amsterdam
21		AM4	Science Park 610, 1098 XH Amsterdam
22		AM5	Schepenbergweg 42, 1105 AT Amsterdam
23		AM6	Amstel Business Park Campus Duivendrechtsekade 80A, 1096 AH Amsterdam
24		AM7	Kuiperbergweg 13, 1101AE Amsterdam
25		AM8	Gyroscoopweg 2E-F, 1042AM Amsterdam
26		EN1	Auke Vleerstraat 1 7521 PE Enschede
27		ZW1	Telfordstraat 3, 8013 RL Zwolle

[Intentionally Blank]

#	Region	Site	Location
28	France	PA1	Paris Nord 2, 167 Rue de la Belle Etoile, 95948 Roissy, CDG Cedex
29		PA2	114 Rue Ambroise Croizat, Saint Denis, 93200
30		PA3	114 Rue Ambroise Croizat, Saint Denis, 93200
31		PA4	110 Bis avenue du Général Leclerc Pantin 93500
32		PA5	45 avenue Victor Hugo, Building 254, Zone EMGP - rue du Mimosa, 93300 Aubervilliers
33		PA6	10 rue Waldeck Rochet Building 520 93300 Aubervilliers
34		PA7	130-136 Boulevard de Verdun, Energy Park 9, 92400 Courbevoie
35		PA8x	110 Bis avenue du Général Leclerc Pantin 93500
36	Spain	MD1	Calle Isabel Colbrand 6-8 Madrid
37		MD2	Calle Valgrande, 6 Alcobendas, Madrid 28108
38		BA1	Carrer de l'Acer 30-32, 08038 Barcelona
39		SA1	Avenida Montes Sierra 48B , 41007 Seville
40	Portugal	LS1	Avenida Severiano Falcão 14, 2685-378 Prior Velho
41	Finland	HE1	Hiomotie 32, 00380 Helsinki
42		HE3	Parrukatu 2, 00570 Helsinki
43		HE4	Myllynkivenkuja 4B, 01620 Vantaa
44		HE5	Sahamyllyntie 4B, 00560 Helsinki
45		HE6	Sinimaentie 12, 02630 Espoo
46		HE7	Sinimaentie 8, 02630 Espoo
47	Sweden	SK1	Mariehällsvägen 36, SE-168 65, BROMMA
48		SK2	Kvastvägen 25-29, SE-128 62, SKÖNDAL Stockholm
49		SK3	Finspångsgatan 48, SE-163 53, SPÅNGA
50	Germany	DU1	Albertstrasse 27, 40233 Düsseldorf
51		FR1	Taubenstrasse 7 – 9, Frankfurt am Main 60313
52		FR2	Kruppstrasse 121-127, Frankfurt 60388
53		FR4	Lärchenstrasse 110, Frankfurt 65933
54		FR5	Kleyerstrasse 90, 60326 Frankfurt
55		FR6	Lärchenstrasse 110, Frankfurt 65933
56		FR7	Gutleutstrasse 310, 60327 Frankfurt am Main
57		MU1	Seidlstrasse 3, Munich 80335
58		MU3	Seidlstrasse 3, Munich DE 80335
59	Bulgaria	SO1	10 5030 Str., Druzhba-1 district 1592 Sofia, Bulgaria
60		SO2	33 Poruchik Nedelcho Bonchev Str.,1528 Sofia

#	Region	Site	Location
61	Switzerland	ZH2	Josefstrasse 225, 8005 Zurich
62		ZH4	Josefstrasse 225, 8005 Zurich
63		ZH5	Allmendstrasse 13, Oberengstringen 8102
64		GV1	6 Rue de la Confederation, CH-1204 Geneva
65		GV2	48, Route du Bois-des-Freres, 1219 Le Lignon
66	Italy	ML2	Via Savona 125 20144 - Milano (MI)
67		ML3	Via Francesco Sforza, 13 20080 - Basiglio (MI)
68	Poland	WA3	Jerozolimskie Avenue 213, 02-222 Warsaw
69	Turkey	IL2	Yukarı Dudullu Mahallesi, Istanbul Dudullu Organize Sanayi Bölgesi, 3 Cd. No:4, 34775 Dudullu Osb/Ümraniye/İstanbul
70	UAE	DX1	F88 – 92 Dubai Production City Sheikh Mohammed Bin Zayed Road, Dubai
71		DX2	Dubai Khazna Datacentre, Meydan, Nad Al Sheba 1, Dubai
72		AD1	Abu Dhabi Khazna Datacentre, Masdar City, Abu Dhabi

The specific control objectives and related control activities included within the scope of this engagement can be found in Section 4 of this document.

Equinix's data center hosting services system environment is an information technology general control (ITGC) 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 Equinix's data center hosting 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.

Subservice Organizations

No subservice organizations were included in the scope of this examination.

Significant Changes During the Review Period

The WA3 data center was placed into operational service at the end of April 2020. The testing of operating effectiveness of the control activities within the Physical Security and Facility and Environmental Security control objectives specific to WA3 were excluded from the scope of this report for the period November 1, 2019, through April 30, 2020 (the period prior to the service go-live for WA3).

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

Functional Areas of Operations

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

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

Equinix's internal leadership focuses on finding new ways to bring innovation, leadership, and quality to support the company's objective to be the interconnection platform for the world's leading businesses. Executive and regional management teams meet regularly to discuss such topics as emerging trends, potential risks to the organization,

and potential new strategies. These teams are composed of a cross functional group of executives to prevent domination by only one or two individuals. The global executive team includes the president and chief executive officer; executive vice president, global operations; chief product officer; chief sales officer; chief technology officer; chief legal and human resources officer; chief strategy and development officer; chief customer and revenue officer; chief financial officer; executive chairman; and senior vice president, chief information officer. Regional managements teams comprised a president, senior vice president of sales, and managing director(s) are in place to oversee the management, strategy, and growth of Equinix in the Americas; EMEA; and Asia-Pacific (AP).

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

Infrastructure

The Data Center Hosting Services system includes the physical infrastructure, power, and data connectivity needed to house customer information systems. Equinix also provides certain physical and environmental security mechanisms to safeguard user entities' assets and data from unauthorized access and environmental threats.

A combination of custom developed, externally supported, and wholly purchased applications are utilized to support the Data Center Hosting Services system. 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 / Resource Support Office (RSO)
Closed circuit television (CCTV) system (various platforms – varies by region / location)	Surveillance camera system used for security monitoring of data centers 24 hours per day; CCTV cameras are positioned throughout the data centers to monitor and track the activity of any person while inside and outside of the data centers	Windows / Linux	Data center facilities / RSO
Building Management System (BMS) (various platforms – varies by region / location)	Building management system used to monitor environmental controls and alert data center personnel to potential issues within the data center, including critical electrical components, power management equipment, heating, ventilation, and air-conditioning (HVAC) equipment, and fire detection and suppression equipment	Windows / Linux	Data center facilities / RSO
Equinix Customer Portal (ECP)	Web-based portal used by customers to manage their access control lists including access change requests and visitor access requests to data center; place orders for IBX data center products and schedule services; and view order statuses, access reports, account information, and review invoices	Windows / Linux	Corporate IT / Network Operations Center (NOC)

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System**	**Physical Location**
Global Service Desk (GSD) and Siebel ticketing systems	Ticketing system used to record, track, and monitor internal and external reported incidents, requests, and notifications applicable to physical and environmental security matters	Windows / Linux	Data center facilities / RSO
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 / RSO
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

Data Management

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

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

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

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.
- Pre-hire reference checks and / or background checks are performed, subject to local laws, for employee candidates as a component of the hiring process.

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.

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.

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 is in place for employees to anonymously report violations, complaints or concerns related to company policies and the code of conduct.
- Management provides internal control performance metrics to the ISMC on an annual basis and documents the metrics in internal control performance dashboards for the ISMC review.

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 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.

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

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 operating 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 decisions related to financing, capital expenditures and expansion

Internal Factors

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

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 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

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

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

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

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

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

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

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

Value	P	HI	PI	BI
0	Not applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0	Not Applicable – Insert 0
1	Improbable occurrence – could not conceivably happened or expect to happen less than once in 100 years.	Negligible – no first aid required	Negligible – negligible damage	Negligible – no direct damage to business delivery (US$0-$135 / €0-100)
2	Possible occurrence – expected to happen once or more every 10 years *(Note: Includes 1 – 10 years).*	Insignificant – slight injury requiring on-site first aid	Insignificant – insignificant damage; structural integrity not affected	Insignificant – minor damage to business delivery; customers not harmed (US$135-$1350 / €100-1000)

Value	P	HI	PI	BI
3	Occasional occurrence – could happen, but rarely. Expected to occur annually or every 6 months.	Slight – one person requiring hospital treatment	Slight – slight damage; structural integrity not affected	Slight – minor damage with single customer affected (US$1350-$13,500 / €1000-10,000)
4	Frequent – could happen monthly / quarterly.	Significant – multiple injuries requiring hospital treatment	Significant – some property damage or loss, including moderate structural damage	Significant – parts of business delivery damaged; multiple customers involved (US$13,500-$135,000 / €10,000-100,000)
5	Regular occurrence – could happen weekly / monthly.	Considerable – death and/or serious injury	Considerable – extensive property damage or loss; structure requires extensive repairs	Considerable – business delivery seriously damaged, >80% customer involved (US$135,000-$1350,000 / €100,000-1,000,000)
6	Common occurrence – could happen daily / weekly.	Catastrophic – multiple deaths and/or serious injuries	Catastrophic – almost total damage or loss; facility must be torn down and replaced	Catastrophic – no business delivery possible (>US$1,350,000 / €1,000,000)

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

Value	PP	IR	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
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

Value	PP	IR	ER
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 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: Controls provide reasonable assurance that physical access to Equinix IBX locations, facility infrastructure platforms, and customer footprint(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. The exterior walls extend from the floor to the ceiling.

Facility and 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. With this level of redundancy, Equinix performs regular preventative maintenance on the equipment with no impact to the user entities. The generators and UPS systems are each inspected for maintenance by facilities personnel, and third-party vendors, and inspection reports are maintained.

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.

[Intentionally Blank]

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 Data Center Hosting Services system. Management obtains or generates and uses relevant internal and external information sources to support the functioning of internal control. Equinix's internal systems supporting the data center hosting services include Dell Blade servers running on Windows and Red Hat Enterprise Linux operating systems. These internal systems are used to:

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

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.

External Communications

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

MONITORING

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.

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
- ISO 22301
- ISO 9001
- Environmental, Energy, Health and Safety Standards: ISO 45001, ISO 50001 and ISO 14001
- Payment Card Industry Data Security Standard (PCI DSS)

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 Data Center Hosting 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 Data Center Hosting Services system to be solely achieved by Equinix's control activities. Accordingly, user entities, in conjunction with the Data Center Hosting Services system, 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 Equinix is notified of changes made to technical or administrative contact information.	Physical Security
User entities are expected to implement controls that ensure the provision and maintenance of facility access list of authorized personnel, vendors, and contractors.	
User entities are expected to implement controls that ensure notification to 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 adherence to the Equinix physical security and safety procedures.	
User entities are expected to implement controls that ensure vendors are informed of the Equinix security 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 the immediate notification of Equinix for 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.	

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Data Center Hosting Services system provided by Equinix. The scope of the testing was restricted to the Data Center Hosting Services system 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 review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

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

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

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

Sampling

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

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

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.

PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Controls 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 policies and procedures exist to help restrict and control access to IBX facilities.	Inspected the physical security policies and procedures to determine that documented policies and procedures were in place to help restrict and control access to data center facilities.	No exceptions noted.
	Data Center Facilities		
1.02	Procedures exist and are followed to establish and make changes to IBX physical access privileges for Equinix employees who have a need to access an IBX.	Observed the access request documentation for a sample of employees hired during the review period to determine that procedures were in place and followed to provision access privileges for data center access for each employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the access removal documentation and the data center physical control system access listings for a sample of terminated employees during the review period to determine that procedures were in place and followed to de-provision IBX access privileges for each employee sampled.	No exceptions noted.
		Inspected the physical security policies and procedures to determine that documented procedures were in place to guide personnel in establishing and making changes to physical access privileges for Equinix employees who had a need to access a data center.	No exceptions noted.
1.03	Procedures exist and are followed to establish and make changes to IBX physical access privileges for customers.	Inquired of the data center managers regarding the customer access procedures for facilities to determine that procedures existed and were followed to establish and make changes to data center physical access privileges for customers.	No exceptions noted.
		Observed the customer access procedures at the data center facilities to determine that procedures were in place to establish and make changes to IBX 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 review period to determine that procedures were followed to establish and make changes to physical access privileges for customers to each facility.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.04	For off-site employees, customers, vendors, and contractors, security or Equinix personnel review valid government issued photo identification prior to allowing access to Equinix facilities.	Inquired of the data center managers regarding the general access procedures for facilities to determine that security or Equinix personnel reviewed a government issued ID for off-site employees, customers, vendors, and contractors, security personnel prior to allowing access to Equinix facilities.	No exceptions noted.
		Observed the visitor access procedures at the data center facilities to determine that security or Equinix personnel reviewed a government issued ID prior to allowing visitors access to each facility.	No exceptions noted.
1.05	New security personnel undergo a formal training program, and their performance is reported and reviewed at least quarterly.	Inquired of the data center managers regarding security personnel training procedures to determine that new security personnel were required to complete a formal training program, and that their performance was reported and reviewed at least quarterly.	No exceptions noted.
		Inspected the confirmation of security guard training completion for a sample of data center facilities to determine that new security training personnel completed a formal training program during the review period for each facility sampled.	No exceptions noted.
		Inspected the security guard performance metrics reports for a sample of data center facilities and quarters during the review period to determine that security personnel performance was reported for each facility and quarter sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.06	Dual control biometric readers, four-digit personal identification numbers and / or proxy cards are in place to help ensure that only authorized individuals have the ability to access the IBX facility, warehouse area, and storage cages. This control shall be applied as and where applicable.	Observed the entrances and doors at the data center facilities to determine that dual control biometric readers, four-digit personal identification numbers and / or proxy cards were in place to restrict access to the facility, warehouse area, and storage cages, where applicable, at each facility.	No exceptions noted.
1.07	Ingress mantraps are in place and administered to help restrict access to IBX facilities to only authorized individuals. Else, there needs to be continuous monitoring of IBX access doors leading to the exterior.	Observed the mantrap entry points and site security monitoring procedures at the data center facilities to determine that ingress mantraps were in place to restrict access the facility and/or access doors leading to the exterior were continuously monitored at each facility.	No exceptions noted.
1.08	Internal and external monitoring of IBX activity is performed through the use of 24x7 security guard personnel and security cameras.	Inquired of the data center managers regarding the internal and external monitoring procedures to determine that internal and external monitoring of data center activity was performed through the use of 24x7 security guard personnel and security cameras.	No exceptions noted.
		Observed the security monitoring procedures at the data center facilities to determine that monitoring of data center activity was performed through the use of security guard personnel and / or security cameras.	No exceptions noted.
		Inspected the facility security guard shift schedule for a sample of data center facilities and months during the review period to determine that security guard personnel were scheduled 24x7 to monitor data center activity for each facility and month sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.09	Each customer has a defined space within the IBX that is physically secured within a locked cage and / or cabinet.	Inquired of the data center managers regarding customer space within the data center facilities to determine that each customer had a defined space within each data center facility that was physically secured within a locked cage and/or cabinet.	No exceptions noted.
		Observed the locked cages and / or cabinets at the data center facilities to determine that customers had defined space that was physically secured within a locked cage and / or cabinet at each facility.	No exceptions noted.
1.10	Customers sign contracts and nondisclosure agreements with Equinix.	Inquired of the standards and compliance senior manager regarding customer contracts to determine that customers were required to have signed contracts and nondisclosure agreements in place with Equinix.	No exceptions noted.
		Observed the contracts and nondisclosure agreements for a sample of new customers onboarded during the review period to determine that signed contracts and nondisclosure agreements were in place for each customer sampled.	No exceptions noted.
1.11	Security surveillance camera logs are recorded and maintained for a minimum of 90 days unless specified otherwise per local country law/regulation.	Inspected the historical surveillance camera logs maintained for a sample of data center facilities to determine that surveillance camera footage was maintained for a minimum of 90 days for each facility sampled, unless specified otherwise per local country law/regulation.	No exceptions noted.
1.12	The IBX data center floor does not have any windows leading to the exterior of the building, where applicable. In case due to the existing infrastructure there are windows and entry points leading to the exterior then they need to be locked from inside or access controlled.	Observed the colocation space at the IBX facilities to determine that data center floors at each of the IBX facilities did not have windows leading to the exterior of the building or in cases where the existing infrastructure did not allow, windows and entry points were locked from the inside or access controlled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.13	Biometric hand scan and / or proxy card access to the IBX is electronically logged and maintained as per data privacy laws. Exceptions or attempts of unauthorized access is tracked and escalated.	Inquired of the data center managers regarding the access logging and escalation procedures for access control systems to determine that biometric hand scan and / or proxy card access to the IBX was electronically logged and maintained, as per data privacy laws, and that exceptions or attempts of unauthorized access were tracked and escalated.	No exceptions noted.
		Inspected the sample historical access control system logs and for a sample of data center facilities and months during the review period to determine that biometric hand scan and / or proxy card access was electronically logged and archived in accordance with data privacy law for each facility and month sampled.	No exceptions noted.
1.14	Technical vendors are given access to data centers and systems only on a need basis and their activities are closely monitored and tracked by the security personnel.	Inquired of the data center managers regarding the technical vendor access procedures to determine that technical vendors were given access to data centers and systems only on a need basis and their activities were closely monitored and tracked by the security personnel.	No exceptions noted.
		Observed the vendor access procedures at the data center facilities to determine that technical vendor access to the data centers and systems was granted on a need basis, and vendor activities were monitored and tracked.	No exceptions noted.
1.15	Pre-hire reference checks are conducted as a component of the new hire process. Employee background checks are performed, subject to local laws.	Observed the reference and background check results for a sample of employees hired during the review period to determine that a pre-hire reference check was conducted and / or a background check was performed, subject to local laws, for each employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.16	Security guards perform a handover exercise upon change of shift.	Inspected the IBX facility security guard shift handover log for a sample of IBXs and dates during the review period to determine security guards performed a handover exercise upon changes of for each IBX facility and date sampled.	No exceptions noted.

FACILITY AND 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 policies and procedures exist to help ensure that IBX facilities have a consistent level of facility and environmental protection.	Inspected the facility and environmental security policies and procedures for a sample of data center facilities to determine that documented policies and procedures were in place to help ensure that data center facilities maintained a consistent level of facility and environmental protection.	No exceptions noted.
	Data Center Facilities		
2.02	IBX facilities are monitored 24x7 by facilities engineers. Equinix has staff in place either on-site or on call 24x7 who are alerted by the BMS for system exceptions.	Inspected the facility operations shift schedules for a sample of data center facilities and months during the review period to determine that facilities personnel were scheduled either on-site or on call 24x7 for each facility and month sampled.	No exceptions noted.
		Inspected the BMS and example alert notifications generated during the review period for a sample of data center facilities to determine that a BMS was in place for alerting facility staff of system exceptions at each facility sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.03	BMS is used to monitor the critical IBX equipment and alert IBX staff of any potential issues.	Observed the BMS in place at the data center facilities to determine that BMS was used to monitor the critical facility equipment and alert staff of potential issues at each facility.	No exceptions noted.
		Inspected the BMS and example alert notifications generated during the review period for a sample of data center facilities to determine that a BMS was in place for alerting IBX staff of system exceptions at each facility sampled.	No exceptions noted.
2.04	Power management equipment for each IBX is in place, which in addition to stand by generators, will include one or more of the following: • The mission critical electrical loads have redundant UPS or critical power supply (CPS) systems • Distributed redundancy achieved through a reserve UPS system • Power management modules to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring, and control of power to the critical customer and Equinix computer loads	Observed the data center facilities to determine that power management equipment was in place including stand-by generators and one or more of the following at each facility: • The mission critical electrical loads have redundant UPS or CPS systems • Distributed redundancy achieved through a reserve UPS system • Power management modules to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring, and control of power to the critical customer and Equinix computer loads	No exceptions noted.
2.05	Scheduled maintenance procedures are performed to test and validate the operation of the power management and environmental systems.	Inspected the most recent UPS inspection reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed to test and validate the operation of the UPS power management systems during the review period for each facility sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent generator inspection reports for a sample of data center facilities to determine that scheduled maintenance procedures were performed to test and validate the operation of the generator power management systems during the review period for each facility sampled.	No exceptions noted.
2.06	Fire detection and suppression equipment is in place to help provide the IBX with ongoing environmental protection.	Observed the data center facilities to determine that fire detection and suppression equipment was in place at each facility.	No exceptions noted.
2.07	Scheduled maintenance procedures are performed to help ensure that fire detection and suppression equipment is working properly.	Observed the inspection tags for a sample of hand-held fire extinguishers at each data center facility to determine that scheduled maintenance was performed to help ensure fire extinguishers were working properly during the review period for each IBX facility fire extinguisher sampled.	No exceptions noted.
		Inspected the most recent fire detection and suppression inspection reports for a sample of data center facilities to determine that fire detection and suppression equipment testing, and validation was performed during the review period for each facility sampled.	No exceptions noted.
2.08	Temperature and humidity is monitored and required temperature is maintained throughout the IBX facilities through the use of air conditioning and ventilation equipment.	Observed the data center facilities to determine that air conditioning, cooling and ventilation equipment was in place to monitor and maintain required temperature and humidity levels at each facility.	No exceptions noted.
2.09	Scheduled maintenance procedures are performed to help ensure that HVAC equipment, cooling equipment, and leak detection sensors are working properly.	Inspected the most recent HVAC inspection report inspection reports for a sample of data center facilities to determine that scheduled maintenance was performed to help ensure that HVAC equipment, cooling equipment, and leak detection sensors was working properly during the review period at each facility sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.10	Equinix maintains leak detection systems surrounding “at risk’” areas to monitor for water within the buildings.	Observed the data center facilities to determine that leak detection systems were maintained to monitor for water within the “at risk” areas of the building at each facility.	No exceptions noted.
2.11	Insurance is in place for IBX locations and equipment.	Inspected the certificates of insurance maintained by Equinix for the data center facilities during the review period to determine that insurance was in place for the data center facilities and equipment.	No exceptions noted.
2.12	Emergency procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the emergency policies and procedures and the security staff procedures to determine to determine that emergency procedures were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected the business recovery plans for a sample of data center sites to determine that a business recovery plan was in place to protect against disruptions caused by an unexpected event for each facility sampled.	No exceptions noted.
2.13	Incident management procedures exist and are tested on regular basis.	Inspected the incident management policies and procedures to determine that an incident management process existed.	No exceptions noted.
		Inspected the most recent completed incident management testing reports for a sample of data center facilities to determine that incident management procedures were tested during the review period for each facility sampled.	No exceptions noted.
2.14	Cables and wires are adequately secured to prevent tampering.	Observed the data center facilities to determine that cables and wires were secured to prevent tampering at each facility.	No exceptions noted.

Section 5

Other Information Provided by Management

EQUINIX'S GLOBAL DATA PRIVACY POSITIONING STATEMENT

This is a positioning statement in relation to data privacy and how Equinix, as a global organization, is managing compliance with data privacy laws in around the work that regulate the handling and controlling of personal data.

Equinix has taken advice from its internal and external legal advisers in each Country where it operates.

Equinix is a global operator of high availability data centers, providing colocation, interconnection and ancillary services to business enterprises in major metropolitan areas around the world.

Equinix's Relationship with Personal Data

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

In this respect, it is Equinix's clear position that such collection, processing, storing and transfers are currently carried out in accordance with:

i. The GDPR, the E-Privacy Directive 2002/58/EC and generally, all applicable data protection laws worldwide;

ii. Equinix's Binding Corporate Rules ("BCRs"), which became the first ever BCRs approved by the European Data Protection Board, consisting of all 28 Member states of the European Union, under the new GDPR regime. Equinix's BCRs allow it to transfer personal data from the European Economic Area ("EEA") and Switzerland to its affiliates across the globe, whilst adhering to the highest standards demanded by EU regulators; and

iii. the EU Model Clauses as approved by the European Commission and which are a set of published standard clauses applicable to data transfers from the EEA and Switzerland to third countries;

and so as to fully guarantee that appropriate legal and other adequate safeguards and measures are in place for the handling of such personal data as described above and personal data within and outside of the Equinix affiliated group of companies.

A "Gold Standard" Global Privacy Program

Whilst the process to have our BCRs approved was complex and time consuming, being the first company globally to have completed this process under the new GDPR regime, not only shows Equinix leading the way in respect of its compliance obligations, but it also serves as a real stamp of quality and accountability against Equinix's Global Privacy Program.

Equinix's Global Privacy Program is well-designed and confirms that all proper safeguards are in place to ensure that we handle personal data correctly and in accordance with applicable data privacy laws.

Whilst Equinix has historically used the EU Model Clauses in its inter-company agreements to facilitate such data transfers from the EEA and Switzerland (which will remain in place), the BCRs provide the added "gold standard" in providing adequate safeguards to enable intra-group transfers to meet operational requirements and to facilitate the transborder flow of data as necessary today to run a global enterprise. This endorsement from the EU for our transborder data flows in how we run our global business if foundational for our own compliance strategy and helping our customers around the world with theirs.

In having its BCRs approved, Equinix has received a declaration of compliance from the EU in relation to the data protection principles laid out by the GDPR. Implementing the BCRs was favoured by Equinix over the EU-U.S. Privacy Shield Framework approach.

Furthermore, as the GDPR refers to BCRs, it recognizes the BCRs as the preferred tool for data flows outside the EEA and Switzerland. As such, it was critical for Equinix that the BCRs provide greater and harmonized protection to the individuals whose personal data is being collected, processed, transferred and are more consistent with Equinix's overall corporate position, which places high importance on data privacy matters and the general integrity of data, including, in this case, personal data.

Data Center Services and Personal Data

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

i. as Equinix (and/or its agents, representatives, suppliers or sub-contractors) has no physical or logical access, use or control, nor does it perform any processing activity in any way or assumes any responsibility over the customer or end-user application data that transits or is stored on the customer owned or controlled server environment ("End-User Data"), such End-User Data is outside the reach of applicable data privacy legislation to Equinix's business;

ii. the GDPR definition of processing includes a key feature of 'disclosure by transmission' and consequently, as Equinix has no logical access to End-User Data, to the extent that such End-User Data contains personal data, Equinix's position is that the transmission of such End-User Data does not constitute processing under applicable GDPR or other applicable data privacy laws because such personal data is not disclosed by transmission to Equinix; and

iii. as a result, Equinix does not perform any processing activity and therefore, it does not assume any legal responsibility as a data processor (or data controller or otherwise) in relation to the End-User Data.

Accordingly, when End-User Data includes personal data, as between Equinix and its customers, Equinix's customers remain responsible as data controllers and as such are the sole part responsible for their own compliance with GDPR and applicable data privacy laws around the world.

The only personal data of customers with respect to which Equinix assumes data privacy responsibilities and to which the statements made above apply are: (i) contact details and related personal information, plus individual biometric data, provided to Equinix for allowing secure access of customer representatives to its data centers, which Equinix handles fully in compliance with applicable data protection regulations, and/or the management of the customer relationship ("CRM"), including via Equinix's global CRM database.

GDPR Compliance and On-going Maintenance of Global Privacy Program

Equinix has undertaken a comprehensive company-wide project to review the application of GDPR to Equinix's business and our Global Privacy Program to implement GDPR. Whilst GPDR compliance is an ongoing obligation, Equinix has achieved a robust and "gold standard" in GPDR compliance and this is demonstrated by becoming the first-ever company to have its BCRs approved under the new GDPR regime.

It is becoming apparent that governments around the world are considering and implementing data privacy regulations modelled after the GDPR, including locations where Equinix does business, such as California and Brazil. The Global Privacy Program is a critical part of the overall Equinix data privacy compliance framework that facilitates delivery of Equinix's global corporate strategy to support our global customers and partners, who look to us to provide the security and trust required around how we operate our global enterprise.

Equinix continues to review its Global Privacy Program on an ongoing basis to remain at the forefront of global privacy compliance.

This positioning statement is not to be taken as or understood as being the provision of legal advice or opinion by Equinix.