| Document Information | |
|---|---|
| **Document Name** | Equinix EMEA B.V. ISO27001 Statement of Applicability (SoA) |
| **Version** | 7.1 |
| **Implementation Date** | 19th February 2020 |
| **Approver** | Director, Operations Enablement EMEA |
| **Document Classification** | Equinix Public |

| Change Log | | | |
|---|---|---|---|
| **Date** | **Version** | **Name** | **Description of Change** |
| 14-Jan-11 | 0.1 | Rohit Advani | New document |
| 28-Jan-11 | 1.0 | Tony Allen | Approval by Management |
| 30-Jan-11 | 1.1 | Rohit Advani | Annual review + updates |
| 30-Jan-12 | 2.0 | Tony Allen | Approval by Management |
| 24-Jan-13 | 2.1 | Rohit Advani | Annual review + updates |
| 28-Jan-13 | 3.0 | Tony Allen | Approval by Management |
| 22-Jan-14 | 3.1 | Rohit Advani | Annual review + updates |
| 27-Jan-14 | 4.0 | Tony Allen | Approval by Management |
| 19-Jan-15 | 4.1 | Rohit Advani | Update as per 2013 standard |
| 25-Jan-15 | 5.0 | Tony Allen | Approval by Management |
| 7-Jan-16 | 5.1 | Rohit Advani | Update to combine all EMEA countries into one SoA |
| 7-Jan-16 | 6.0 | Keith Tipson | Approval by Management |
| 24-Jun-18 | 7.0 | Rohit Advani | Template updated to standardize globally |
| 19-Feb-20 | 7.1 | Rohit Advani | Updates made to scope statement and sections 10.1.2, 12.1.4, 12.2.1, 13.1.1, 13.1.2, 13.1.3, 14.1.1, 18.1.5 |

## Scope Statement

This Statement of Applicability and implemented Information Security Management System applies to the following scope:

***The Information Security Management System (ISMS) provides the information security framework for the activities relating to the provision, maintenance and operation of 24x7 International Business Exchange (IBX) data centres and IBX Services (Colocation, Smart-Hands, Cross Connects, Flexspace and where relevant Managed Services) and related support services from Equinix's data centre locations across the EMEA region***

The implemented ISMS and related control measures are applicable to all business processes of Equinix EMEA IBX's and apply to all employees, permanent or temporary.

# Equinix EMEA ISO27001 Statement of Applicability

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| **Information Security Policies A5** | **5.1** | **Management direction for information security** | | | | |
| | **Objective:** | **To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.** | | | | |
| | 5.1.1 | Policies for information security | Y | Y | To achieve the control objective | EMEA Information Security Policy<br>Country Employee Handbook<br>Global IBX Physical Security Policies |
| | 5.1.2 | Review of the policies for information security | Y | N | To achieve the control objective | Global IBX Physical Security Policies |
| **Organization of Information Security A6** | **6.1** | **Internal Organization** | | | | |
| | **Objective:** | **To establish a management framework to initiate and control the implementation and operation of information security within the organization.** | | | | |
| | 6.1.1 | Information security roles and responsibilities | Y | Y | To achieve the control objective | EMEA Information Security Policy<br>EMEA ISMS Manual<br>Function descriptions<br>EMEA Employee handbook |
| | 6.1.2 | Segregation of duties | Y | Y | To achieve the control objective | Global IBX Physical Security Policies<br>Global Standard Job Descriptions for Security<br>IBX Risk Assessments |
| | 6.1.3 | Contact with authorities | Y | Y | To achieve the control objective | EMEA ISMS manual<br>IBX Business Recovery Plan<br>Country Compliance Annex<br>IBX Threat & Risk Assessments<br>IBX Emergency Contact List (ECL) |
| | 6.1.4 | Contact with special interest groups | Y | Y | To achieve the control objective | EMEA ISMS manual<br>Country Compliance Annex<br>IBX Risk Assessment<br>Global Business Continuity Exercise Program<br>Global Security Threat Level Procedure |
| | 6.1.5 | Information security in project management | Y | N | To achieve the control objective | Global Change Management Process (CMR)<br>Global IBX Security Design Standard Division 280000<br>Permit to Work |
| | **6.2** | **Mobile devices and teleworking** | | | | |
| | **Objective:** | **To ensure the security of teleworking and use of mobile devices.** | | | | |
| | 6.2.1 | Mobile device policy | Y | N | To achieve the control objective | Global IT Acceptable Use Policy<br>IS Code of Conduct |
| | 6.2.2 | Teleworking | Y | N | To achieve the control objective | Global IT Acceptable Use Policy |
| **Human Resources Security A7** | **7.1** | **Prior to Employment** | | | | |
| | **Objective:** | **To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.** | | | | |
| | 7.1.1 | Screening | Y | Y | To achieve the control objective | EMEA Staff Recruitment Process<br>Equinix Global Background Screening Policy & Country Addendums |
| | 7.1.2 | Terms and conditions of employment | Y | Y | To achieve the control objective | Staff recruitment process<br>Country Employee Handbook<br>HR Employment Contracts |
| | **7.2** | **During Employment** | | | | |
| | **Objective:** | **To ensure that employees and contractors are aware of and fulfil their information security responsibilities.** | | | | |
| | 7.2.1 | Management responsibilities | Y | Y | To achieve the control objective | Letter of Intent<br>EMEA Information Security Policy |
| | 7.2.2 | Information security awareness, education and training | Y | Y | To achieve the control objective | EMEA Staff Recruitment Process<br>GPL and Org-specific SharePoint<br>Global Equinix Learning Centre - Security Awareness Training |
| | 7.2.3 | Disciplinary process | Y | N | To achieve the control objective | Global Disciplinary Policy<br>Country Employee handbook |
| | **7.3** | **Termination or change of employment** | | | | |
| | **Objective:** | **To protect the organization's interests as part of the process of changing or terminating employment.** | | | | |
| | 7.3.1 | Termination or change of employment responsibilities | Y | Y | To achieve the control objective | EMEA Leavers Process |

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| Asset management **A8** | **8.1** | **Responsibility for Assets** | | | | |
| | **Objective:** | **To identify organizational assets and define appropriate protection responsibilities.** | | | | |
| | 8.1.1 | Inventory of assets | Y | N | To achieve the control objective | ISMS Asset Management Policy<br>MAXIMO<br>New Hire checklist<br>EMEA Leavers checklist<br>IT Asset Management Tool |
| | 8.1.2 | Ownership of assets | Y | N | To achieve the control objective | ISMS Asset Management Policy<br>MAXIMO<br>IT Asset Management Tool |
| | 8.1.3 | Acceptable use of assets | Y | Y | To achieve the control objective | ISMS Asset Management Policy<br>Global IS Code of Conduct<br>MAXIMO - Asset Management System<br>Global IT Acceptable Use Policy |
| | 8.1.4 | Return of assets | Y | Y | To achieve the control objective | ISMS Asset Management Policy<br>EMEA Leavers Process<br>EMEA IT Form |
| | **8.2** | **Information classification** | | | | |
| | **Objective:** | **To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.** | | | | |
| | 8.2.1 | Classification of information | Y | Y | To achieve the control objective | Global Data Classification, Labelling, and Handling Policy<br>Global Document Management Process |
| | 8.2.2 | Labelling of information | Y | Y | To achieve the control objective | Global Data Classification, Labelling, and Handling Policy |
| | 8.2.3 | Handling of assets | Y | Y | To achieve the control objective | Global Data Classification, Labelling, and Handling Policy<br>Global IT Acceptable Use Policy |
| | **8.3** | **Media handling** | | | | |
| | **Objective:** | **To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.** | | | | |
| | 8.3.1 | Management of removable media | Y | Y | To achieve the control objective | Global IT Acceptable Use Policy<br>Global IS code of conduct<br>EMEA Media Disposal Process<br>Global Outbound Shipment Process |
| | 8.3.2 | Disposal of media | Y | N | To achieve the control objective | Global IT Acceptable Use Policy<br>Global IS code of conduct<br>EMEA Media Disposal Process<br>Global Outbound Shipment Process |
| | 8.3.3 | Physical media transfer | Y | Y | To achieve the control objective | Global IT Acceptable Use Policy<br>Global IS code of conduct<br>EMEA Media Disposal Process<br>Global Outbound Shipment Process |
| | | | | | | |
| | **9.1** | **Business requirements of access control** | | | | |
| | **Objective:** | **To limit access to information and information processing facilities.** | | | | |
| | 9.1.1 | Access control policy | Y | Y | To achieve the control objective | Global Logical Access Policy<br>Global IT Acceptable Use Policy<br>Global IBX Physical Security Policies<br>EMEA Information Security Policy |
| | 9.1.2 | Access to networks and network services | Y | Y | To achieve the control objective | Acceptable Use Policy<br>IS Code of Conduct<br>Country Employee Handbook<br>EMEA Information Security Policy |
| | **9.2** | **User Access Management** | | | | |
| | **Objective:** | **To ensure authorized user access and to prevent unauthorized access to systems and services.** | | | | |
| | 9.2.1 | User registration and de-registration | Y | Y | To achieve the control objective | Global Physical Security Policies<br>EMEA Information Security Policy |
| | 9.2.2 | User access provisioning | Y | Y | To achieve the control objective | Global IBX Physical Security Policies<br>EMEA Staff Recruitment Process<br>EMEA Leavers Process |
| | 9.2.3 | Management of privileged access rights | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| **Access Control A9** | 9.2.4 | Management of secret authentication information of users | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |
| | 9.2.5 | Review of user access rights | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |
| | 9.2.6 | Removal or adjustment of access rights | Y | Y | To achieve the control objective | EMEA Leavers Process<br>EMEA IT Form |
| | **9.3** | **User Responsibilities** | | | | |
| | **Objective:** | **To make users accountable for safeguarding their authentication information.** | | | | |
| | 9.3.1 | Use of secret authentication information | Y | Y | To achieve the control objective | Global IBX Physical Security Policies<br>EMEA Information Security Policy<br>Global Acceptable Use Policy<br>Global Password Policy |
| | **9.4** | **System and application access control** | | | | |
| | **Objective:** | **To prevent unauthorized access to systems and applications.** | | | | |
| | 9.4.1 | Information access restriction | Y | N | To achieve the control objective | Global Logical Access Policy<br>Global IBX Physical Security Policies |
| | 9.4.2 | Secure log-on procedures | Y | Y | To achieve the control objective | Global Logical Access Policy<br>EMEA Information Security Policy |
| | 9.4.3 | Password management system | Y | N | To achieve the control objective | Global Password Policy |
| | 9.4.4 | Use of privileged utility programs | Y | N | To achieve the control objective | Global Logical Access Policy<br>EMEA Information Security Policy |
| | 9.4.5 | Access control to program source code | N/A | N | No source code nor software or system development activities in the ISMS scope | Equinix does not develop its own software |
| | | | | | | |
| **Cryptography A10** | **10.1** | **Cryptographic controls** | | | | |
| | **Objective:** | **To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.** | | | | |
| | 10.1.1 | Policy on the use of cryptographic controls | Y | N | To achieve the control objective | Global Encryption Policy |
| | 10.1.2 | Key management | N/A | N | Encryption/Cryptographic key management, implementation or development activities not in the ISMS scope. | |
| | | | | | | |
| **Physical and Environmental Security A11** | **11.1** | **Secure Areas** | | | | |
| | **Objective:** | **To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.** | | | | |
| | 11.1.1 | Physical security perimeter | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |
| | 11.1.2 | Physical entry controls | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |
| | 11.1.3 | Securing offices, rooms and facilities | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |
| | 11.1.4 | Protecting against external and environmental threats | Y | Y | To achieve the control objective | Global IBX Physical Security Policies |
| | 11.1.5 | Working in secure areas | Y | Y | To achieve the control objective | Global IBX Physical Security Policies<br>EMEA Health & Safety Policies and Processes |
| | 11.1.6 | Delivery and loading areas | Y | Y | To achieve the control objective | Global IBX Physical Security Policies<br>Global Inbound Shipment Process<br>Global Outbound Shipment Process |
| | **11.2** | **Equipment** | | | | |
| | **Objective:** | **To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.** | | | | |
| | 11.2.1 | Equipment siting and protection | Y | Y | To achieve the control objective | Global Operations Engineering Policies and Procedures<br>Global IBX Physical Security Policies<br>CCTV Policy - EMEA<br>IBX CCTV Plans |
| | 11.2.2 | Supporting utilities | Y | Y | To achieve the control objective | Global Operations Engineering Policies and Procedures<br>Construction Design Standards / Equipment SOPs<br>Global IBX Physical Security Policies |
| | 11.2.3 | Cabling security | Y | Y | To achieve the control objective | Global Cabling Standards |
| | 11.2.4 | Equipment maintenance | Y | Y | To achieve the control objective | Permit to Work Process |
| | 11.2.5 | Removal of assets | Y | Y | To achieve the control objective | Global Outbound Shipment Process<br>Global IT Information Security Data Classification, Labelling and Handling Policy<br>Global IT Acceptable Use Policy<br>IS Code of Conduct |

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| | 11.2.6 | Security of equipment and assets off-premises | Y | Y | To achieve the control objective | Global IBX Physical Security Policies<br>Global CCTV Policy<br>IBX CCTV Plan<br>Construction Design Standards / Equipment SOPs |
| | 11.2.7 | Secure disposal or reuse of equipment | Y | N | To achieve the control objective | Global IT Information Security Data Classification, Labelling and Handling Policy<br>EMEA Media Disposal Process |
| | 11.2.8 | Unattended user equipment | Y | Y | To achieve the control objective | Global IT Acceptable Use Policy<br>IS Code of Conduct |
| | 11.2.9 | Clear desk and clear screen policy | Y | Y | To achieve the control objective | Global IT Acceptable Use Policy<br>IS Code of Conduct |
| | | | | | | |
| **Operations Security A12** | **12.1** | **Operational Procedures and responsibilities** | | | | |
| | **Objective:** | **To ensure the correct and secure operation of information processing facilities.** | | | | |
| | 12.1.1 | Documented operating procedures | Y | N | To achieve the control objective | Policies, Processes, Procedures and Work instructions<br>Published in Global Process Library (GPL) |
| | 12.1.2 | Change Management | Y | N | To achieve the control objective | Global Permit to Work Process<br>Global Change Management Process (CMR) |
| | 12.1.3 | Capacity management | Y | N | To achieve the control objective | CapLogix Application<br>Global Capacity Management Procedures<br>Global Change Management Process (CMR) |
| | 12.1.4 | Separation of development, test and operations facilities | N/A | N | No source code nor software or system development or test activities in the ISMS scope | |
| | **12.2** | **Protection from malware** | | | | |
| | **Objective:** | **To ensure that information and information processing facilities are protected against malware.** | | | | |
| | 12.2.1 | Controls against malware | N/A | N | No malware control activities in the ISMS scope. This function is outsourced to Equinix Inc. IT department which acts as a third party for Equinix EMEA B.V. | Performed by a third party for Equinix EMA B.V.<br>Global IT Anti-virus and Malware Policy<br>Anti-virus installed on PCs and Servers<br>IS Code of Conduct<br>Global IT Applications and Tools |
| | **12.3** | **Backup** | | | | |
| | **Objective:** | **To protect against loss of data.** | | | | |
| | 12.3.1 | Information backup | Y | Y | To achieve the control objective | EMEA Information Security Policy<br>Global IT Data Backup and Retention Policy<br>CCTV and Access Log Backups |
| | **12.4** | **Logging and monitoring** | | | | |
| | **Objective:** | **To record events and generate evidence.** | | | | |
| | 12.4.1 | Event logging | Y | N | To achieve the control objective | Building Monitoring System (BMS) event logs<br>IBX Access Logs<br>IBX Visitor Logs<br>IBX Key Logs |
| | 12.4.2 | Protection of log information | Y | N | To achieve the control objective | EMEA Information Security Policy |
| | 12.4.3 | Administrator and operator logs | Y | N | To achieve the control objective | EMEA Information Security Policy |
| | 12.4.4 | Clock synchronisation | Y | N | To achieve the control objective | EMEA Information Security Policy |
| | **12.5** | **Control of operational software** | | | | |
| | **Objective:** | **To ensure the integrity of operational systems.** | | | | |
| | 12.5.1 | Installation of software on operational systems | Y | N | To achieve the control objective | Global Acceptable Use Policy |
| | **12.6** | **Technical vulnerability management** | | | | |
| | **Objective:** | **To prevent exploitation of technical vulnerabilities.** | | | | |
| | 12.6.1 | Management of technical vulnerabilities | Y | N | To achieve the control objective | Global Patch Management Policy |
| | 12.6.2 | Restrictions on software installation | Y | N | To achieve the control objective | Global Acceptable Use Policy |
| | **12.7** | **Information systems audit considerations** | | | | |
| | **Objective:** | **To minimise the impact of audit activities on operational systems.** | | | | |
| | 12.7.1 | Information systems audit controls | Y | N | To achieve the control objective | Change Logs - Access Control System<br>Change Logs - CCTV Management System |
| | | | | | | |
| | **13.1** | **Network security management** | | | | |

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| **Communications Security A13** | **Objective:** | **To ensure the protection of information in networks and its supporting information processing facilities.** | | | | |
| | 13.1.1 | Network controls | N/A | N | No network activities in the ISMS scope. Performed by Equinix Inc. IT which is a third party for Equinix EMEA B.V. | Performed by a third party for Equinix EMEA B.V.<br>Global VPN Policy<br>Global Logical Access Policy |
| | 13.1.2 | Security of network services | N/A | N | No network activities in the ISMS scope. Performed by Equinix Inc. IT which is a third party for Equinix EMEA B.V. | Performed by a third party for Equinix EMEA B.V.<br>Global VPN Policy<br>Global Logical Access Policy |
| | 13.1.3 | Segregation in networks | N/A | N | No network activities in the ISMS scope. Performed by Equinix Inc. IT which is a third party for Equinix EMEA B.V. | Performed by a third party for Equinix EMEA B.V.<br>Access Control, BMS and CCTV network separate from the Corporate network.<br>LAN Diagram showing segregation. |
| | **13.2** | **Information transfer** | | | | |
| | **Objective:** | **To maintain the security of information transferred within an organization and with any external entity.** | | | | |
| | 13.2.1 | Information transfer policies and procedures | Y | N | Equinix does not exchange information over public networks | Information Security Policy EMEA |
| | 13.2.2 | Agreements on information transfer | Y | N | Equinix does not exchange information over public networks | Information Security Policy EMEA |
| | 13.2.3 | Electronic messaging | Y | N | Equinix does not exchange information over public networks | Global Acceptable Use Policy |
| | 13.2.4 | Confidentiality or nondisclosure agreements | Y | Y | To achieve the control objective | Non-Disclosure Agreements<br>Master Country Agreements<br>Standard Vendor Contracts<br>Country Employee Handbook |
| | | | | | | |
| **System Acquisition Development and Maintenance A14** | **14.1** | **Security Requirements of Information Systems** | | | | |
| | **Objective:** | **To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.** | | | | |
| | 14.1.1 | Information security requirements analysis and specification | Y | N | To achieve the control objective | Business Requirement Documents (BRD),<br>Information Security Policy EMEA<br>Global Equinix Inc. IT Policies |
| | 14.1.2 | Securing application services on public networks | N/A | N | Equinix does not exchange information over public networks | |
| | 14.1.3 | Protecting application services transactions | N/A | N | No E-Commerce environment available | |
| | **14.2** | **Security in development and support processes** | | | | |
| | **Objective:** | **To ensure that information security is designed and implemented within the development lifecycle of information systems.** | | | | |
| | 14.2.1 | Secure development policy | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.2 | System change control procedures | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.3 | Technical review of applications after operating platform changes | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.4 | Restrictions on changes to software packages | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.5 | Secure system engineering principles | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.6 | Secure development environment | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.7 | Outsourced development | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.8 | System security testing | N/A | N | No source code nor software or system development activities in the ISMS scope | |
| | 14.2.9 | System acceptance testing | N/A | N | No system acceptance testing activities in the ISMS scope | |
| | **14.3** | **Test data** | | | | |
| | **Objective:** | **To ensure the protection of data used for testing.** | | | | |
| | 14.3.1 | Protection of test data | N/A | N | No test data activities in the ISMS scope | |
| | | | | | | |
| | **15.1** | **Information security in supplier relationships** | | | | |
| | **Objective:** | **To ensure protection of the organization's assets that is accessible by suppliers.** | | | | |
| | 15.1.1 | Information security policy for supplier relationships | Y | Y | To achieve the control objective | Service Level Agreements in Vendor Contracts<br>IBX Risk Assessment<br>Global Permit to Work Process<br>General Terms and Conditions |

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| **Supplier Relationships A15** | 15.1.2 | Addressing security within supplier agreements | Y | Y | To achieve the control objective | New Vendor Registration Form<br>Non-Disclosure Agreements (NDA)<br>Vendor Contracts<br>Global Permit to Work Process<br>General Terms and Conditions |
| | 15.1.3 | Information and communication technology supply chain | Y | Y | To achieve the control objective | Vendor Contracts<br>Permit to Work Process |
| | **15.2** | **Supplier service delivery management** | | | | |
| | **Objective:** | **To maintain an agreed level of information security and service delivery in line with supplier agreements.** | | | | |
| | 15.2.1 | Monitoring and review of supplier services | Y | Y | To achieve the control objective | EMEA Procurement Processes / COUPA |
| | 15.2.2 | Managing changes to supplier services | Y | Y | To achieve the control objective | EMEA Procurement Processes / COUPA |
| | | | | | | |
| **Information Security Incident Management A16** | **16.1** | **Management of information security incidents and improvements** | | | | |
| | **Objective:** | **To ensure a consistent and effective approach to the management of information securityincidents, including communication on security events and weaknesses.** | | | | |
| | 16.1.1 | Responsibilities and procedures | Y | Y | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy |
| | 16.1.2 | Reporting information security events | Y | Y | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy |
| | 16.1.3 | Reporting information security weaknesses | Y | N | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy |
| | 16.1.4 | Assessment of and decision on information security events | Y | N | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy |
| | 16.1.5 | Response to information security incidents | Y | N | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy |
| | 16.1.6 | Learning from information security incidents | Y | N | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy<br>Country Information Security Working Committee<br>EMEA Annual Management review<br>Post Incident Report (PIR) and Initial Incident Report (IIR) |
| | 16.1.7 | Collection of evidence | Y | N | To achieve the control objective | Global Incident Reporting Management Policy<br>Global IBX Security Incident Management Policy<br>Remedy Application<br>CCTV Recordings<br>Access Logs<br>Access Alarms (Intrusion Detection Alarms)<br>Emails / Photographs<br>SharePoint<br>Box |
| | | | | | | |
| **Information Security Aspects of Business Continuity Management A17** | **17.1** | **Information security continuity** | | | | |
| | **Objective:** | **Information security continuity shall be embedded in the organization's business continuity management systems.** | | | | |
| | 17.1.1 | Planning information security continuity | Y | Y | To achieve the control objective | IBX Business Continuity Program Policy<br>IBX Business Continuity Program Procedure<br>IBX Business Recovery Plan<br>IBX Risk Assessment<br>Business Impact Assessments<br>IBX Business Continuity Exercises Planning within MAXIMO<br>IBX Business Continuity Exercise Report<br>IBX Business Continuity Exercise Program |
| | 17.1.2 | Implementing information security continuity | Y | Y | To achieve the control objective | IBX Business Recovery Plan<br>IBX Risk Assessment<br>Business Impact Assessments<br>IBX Business Continuity Exercises Planning within MAXIMO<br>IBX Business Continuity Exercise Report<br>IBX Business Continuity Exercise Program |
| | 17.1.3 | Verify, review and evaluate information security continuity | Y | Y | To achieve the control objective | EMEA IBX Business Continuity Exercise Report<br>IBX Business Continuity Exercise Program<br>Internal Audit Process<br>EMEA Internal Audit Report |

| ISO 27001:2013 - Annex A 14 Control Objectives (114 Controls) | | | Control Selected? | Risk Relation? | Justification for Inclusion or Exclusion | Evidence of Implementation |
|---|---|---|---|---|---|---|
| **Clause** | **Sec** | **Control Objective** | | | | |
| | **17.2** | **Redundancies** | | | | |
| | **Objective:** | **To ensure availability of information processing facilities.** | | | | |
| | 17.2.1 | Availability of information processing facilities | Y | Y | To achieve the control objective | IBX Business Recovery Plan<br>IBX Threat & Risks Assessment<br>Business Impact Assessments |
| | | | | | | |
| **Compliance**<br>**A18** | **18.1** | **Compliance with legal and contractual requirements** | | | | |
| | **Objective:** | **To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.** | | | | |
| | 18.1.1 | Identification of applicable legislation and contractual requirements | Y | Y | To achieve the control objective | Country Compliance Annexes on GPL |
| | 18.1.2 | Intellectual property rights | Y | N | To achieve the control objective | Global Intellectual Property Rights Policy<br>Acceptable Use policy<br>Country Employee Handbooks |
| | 18.1.3 | Protection of records | Y | N | To achieve the control objective | Global Records Management Policy<br>Global Records Retention Schedule<br>Global IT Information Security Data Classification, Labelling and Handling Policy |
| | 18.1.4 | Privacy and protection of personally identifiable information | Y | N | To achieve the control objective | Country Compliance Annex<br>Country Employee Handbook<br>GDPR Framework implemented by Privacy Office<br>Equinix Privacy Office Charter<br>Equinix Data Privacy Positioning Statement |
| | 18.1.5 | Regulation of cryptographic controls | N/A | N | Encryption/Cryptographic key management, implementation or development activities not in the ISMS scope. | |
| | **18.2** | **Information security reviews** | | | | |
| | **Objective:** | **To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.** | | | | |
| | 18.2.1 | Independent review of information security | Y | Y | To achieve the control objective | EMEA External IT Services Audit Protocol<br>EMEA Internal Audit Policy<br>EMEA Internal Audit Report Template |
| | 18.2.2 | Compliance with security policies and standards | Y | Y | To achieve the control objective | EMEA Management Review Process<br>EMEA Internal Audit Policy<br>EMEA Internal Audit Report Template |
| | 18.2.3 | Technical compliance review | Y | Y | To achieve the control objective | EMEA Internal Audit Policy<br>EMEA Internal Audit Report Template |