SOC 2 Report

interxion™

Interxion Denmark ApS Service Organisation Controls (SOC) 2 Report

Report on Interxion Denmark ApS description of its cloud and carrier colocation data centre services on the suitability of the design and operating effectiveness of its controls relevant to security and availability throughout the period January 1, 2016 to December 31, 2016

www.interxion.com
customer.services@interxion.com

International Headquarters
Main: + 44 207 375 7070
Email: hq.info@interxion.com

European Customer Service Centre (ECSC)
Toll free Europe: + 800 00 999 222 / Toll free US: 185 55 999 222
Email: customer.services@interxion.com

interxion™

Contents

1 Section I: Management Statement of Interxion Denmark ApS

We have prepared the accompanying *"Interxion's cloud and carrier colocation data centre services system operated in Denmark for the period January 1, 2016 to December 31, 2016* " (Description) of Interxion Denmark ApS (Service Organization) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* updated as of July 1, 2015 (the description criteria). The description is intended to provide users with information about the cloud and carrier colocation data centre services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in TSP section 100, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

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

a. the Description fairly presents the System throughout the period January 1, 2016 to December 31, 2016, based on the following description criteria:
    i. The Description contains the following information:
        (1) The types of services provided.
        (2) The components of the system used to provide the services, which are the following:
            - Infrastructure. The physical structures, IT, and other hardware components of a system (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
            - Software. The application programs and IT systems that supports application programs (operating systems, middleware, and utilities).
            - People. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers).
            - Procedures. The automated and manual procedures[1].
            - Data. Transaction streams, files, databases, tables, and output used or processed by the system).
        (3) The boundaries or aspects of the system covered by the description.
        (4) For information provided to, or received from, subservice organizations or other parties
            (a) How such information is provided or received; the role of the subservice organization or other parties
            (b) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
    (5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
        (a) Complementary user-entity controls contemplated in the design of the Interxion Denmark ApS / cloud and carrier colocation data centre services system.
        (b) When the inclusive method is used to present a subservice organization, controls at

[1] The description of the procedures of the system includes those by which services are provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, delivered, and reports and other information prepared.

the subservice organization

(6) If the service organization presents the subservice organization using the carve-out method:

(a) The nature of the services provided by the subservice organization

(b) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.

(8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the Description.

ii. The Description does not omit or distort information relevant to the service organization's system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria were met if the controls operated as described throughout the period January 1, 2016 to December 31, 2016.

c. the Interxion Denmark ApS controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Ballerup, Denmark, February 10, 2017

Peder Bank
Managing Director

Morten Tidemand
Manager Operations

Ernst & Young Accountants LLP
Antonio Vivaldistraat 150
1083 HP AMSTERDAM
Postbus 7883
1008 AB Amsterdam

Tel: +31 88 40 70903
Fax: +31 88 40 71005
ey.com

2 Section II: Independent Service Auditor's Assurance Report

To Management of Interxion Denmark ApS

Scope

We have examined Interxion Denmark ApS' accompanying *"Interxion's cloud and carrier colocation data centre services system operated in Denmark for the period January 1, 2016 to December 31, 2016"* (Description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* updated as of July 1, 2015 (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in the AICPA's TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) throughout the period January 1, 2016 to December 31, 2016.

The information in the accompanying 'Other Information Provided by Interxion Denmark ApS' is presented by management of Interxion Denmark ApS to provide additional information and is not part of Interxion Denmark ApS' Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Interxion Denmark ApS responsibilities

Interxion Denmark ApS has provided the accompanying assertion titled "*Management Statement of Interxion Denmark ApS*" (Assertion) about the fairness of the presentation of the Description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Interxion Denmark ApS is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with Dutch Law and International Standard on Assurance Engagements 3000, 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Our examination was also performed in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material

Building a better working world

Ernst & Young Accountants LLP
Antonio Vivaldistraat 150
1083 HP AMSTERDAM
Postbus 7883
1008 AB Amsterdam

Tel: +31 88 40 70903
Fax: +31 88 40 71005
ey.com

respects, (1) the Description is fairly presented based on the description criteria, and (2) the controls described therein are suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2016 to December 31, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls, involves performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the Description. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are independent of Interxion Denmark ApS in accordance with the ViO (Code of Ethics for Professional Accountants, a regulation with respect to independence) and other relevant independence regulations in the Netherlands. Furthermore we have complied with the VGBA (Dutch Code of Ethics) and with the independence and other ethical requirements set forth in Code of Ethics for Professional Accountants of the International Ethics Standards Board for Accountants (the IESBA Code).

We apply the International Standard on Quality Control Quality Control 1 (ISQC 1) for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements, and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. 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 or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria

a) the Description fairly presents the system that was designed and implemented throughout the period January 1, 2016 to December 31, 2016.

Ernst & Young Accountants LLP
Antonio Vivaldistraat 150
1083 HP AMSTERDAM
Postbus 7883
1008 AB Amsterdam

Tel: +31 88 40 70903
Fax: +31 88 40 71005
ey.com

b) the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2016 to December 31, 2016.
c) the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 1, 2016 to December 31, 2016.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying "Description of Criteria, Controls, Tests and Results of Tests" (Description of Tests and Results).

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Interxion Denmark ApS, user entities of Interxion Denmark ApS' system, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

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

Amsterdam, February 10, 2017

Ernst & Young Accountants LLP

M. van Helden MSc RE
Manager

drs. D. Houtekamer RE
Executive Director

3 Section III: Interxion's cloud and carrier colocation data centre services system operated in Denmark for the period January 1, 2016 to December 31, 2016

3.1 Introduction to Interxion

3.1.1 Interxion

Interxion is organised around Interxion Holding N.V. (NYSE: INXN) and supported by separate local Interxion entities in 11 countries in Europe. The Interxion senior management team brings global experience and knowledge to the roles of business leaders, financial managers, marketing heads and legal experts.

Interxion entities are supported by a Major Accounts team, where the Interxion customer base is divided into high-growth market segments, including financial services, cloud and managed services providers, digital media and carriers. Customers in these target markets enable the expansion of existing communities of interest and build new, communities of interest within the data centre.

Each local Interxion entity has its own profit and loss statement and is managed by a Managing Director to help ensure the operational and commercial management of their customers. Interxion Denmark ApS is a fully-owned subsidiary of InterXion Operational B.V.

3.1.2 Background

Interxion provides cloud and carrier neutral colocation data centre services in Europe through 40 data centres across 11 countries. The head office is in Amsterdam, The Netherlands, and Interxion operates in the major metropolitan areas of Europe including London, Frankfurt, Paris and Brussels. Data centres are located close to city centres and help ensure they have excellent power availability and connectivity. Interxion houses more than 500 carriers and Internet service providers and 20 European Internet exchanges.

Cloud and carrier neutral means the data centre is entirely independent of any network, hardware or software vendor, and colocation means a data centre where equipment space, power and cooling are available for rental. Interxion's cloud and carrier neutral colocation data centre services offer space, power, cooling, data cabling and other services, such as 'Hands & Eyes' (proximity service) and dark fibre connectivity.

Interxion Denmark ApS was founded in 1999 and its cloud and carrier neutral colocation data centre services are provided in their data centres. Interxion Denmark ApSgeographic accessibility allows comprehensive cable infrastructure access to worldwide telecommunications networks.

3.1.3 Central Organisation

On HQ level the following departments operate together to provide a central hub and support for their local resources, these are:-

HQ ICT –HQ Information Communication Technology

HQ HR – HQ Human Resources

HQ ECSC – HQ European Customer Service Centre

DT&EG - Data Centre Technology & Engineering Group

3.1.3.1 Information Communication Technology (ICT)

Interxion HQ Information Communication & Technology (hereafter HQ ICT) is responsible for information technology related hardware and software assets supporting Interxion. Network management, including access to the network, falls under HQ ICT responsibility. For locally implemented server hardware and software assets by the local organisation, HQ ICT supplies ICT services for access management to the

network, backup, security and other ICT related solutions where the owner and responsibility remains with the local organization.

3.1.3.2 **HQ HR**

Interxion Human Resources (hereafter HQ HR) are managed locally operating within a framework largely set by the HQ HR department that is then tailored where necessary to account for local legislation, custom and practice. Wherever possible central management frameworks are provided for use by all countries within the Interxion operation. These frameworks (such as remuneration, performance management, benefits (private healthcare insurance and pensions), recruitment and background / security checking are all mandated and controlled by central HQ HR policy. Some however may vary at the procedural level to take into account the aforementioned legislative, local customs and / or variations in local practice.

Interxion ethics and behaviours are managed centrally with all employees having to sign a Confirmation of Receipt indicating that they are aware of the companywide Acceptable Use Policy (AUP) and Code of Conduct (CoC) soon after the commencement of their employment with the organisation. The CoC is an extensive e-learning module (with an exam at the end) that all employees must take and successfully pass. From this all employees are clear on what they are accountable for in their role, the integrity Interxion expects them to exhibit and the ethics they should be demonstrating in all Interxion business activity.

There is also a framework for functional training that is managed at HQ HR level. Training is based upon the function an employee carries out. Relevant qualifications are maintained and improved as appropriate. There are regular cross country HR meetings to ensure all countries are made aware of the agreed HQ HR policies and given an opportunity to state where central HR policy cannot be applied for the reasons given above.

Due to the nature of Interxion's business employee inductions are carried out at country level. This means that whilst acceptable use of Interxion systems, assets and data are controlled by the central AUP and CoC, individual differences in each country from a procedural level (for instance physical security and fire drills etc.) are managed in the local induction. HR employee data is recorded securely and managed and maintained centrally.

3.1.3.3 **European Customer Service Centre (ECSC)**

Interxion provides the European Customer Service Centre (hereafter ECSC) in London as the single point of contact (SPOC) for Interxion customers, 24x365 from the UK. Comprised of experienced professionals trained in the Information Technology Infrastructure Library (ITILv3) standard, the ECSC team provides native language support in English, French, Spanish and German. In addition to being the single point of contact for customers, the ECSC provides removed monitoring for data centres for critical alarms, providing a second pair of eyes in addition to local monitoring.

The ECSC coordinates the preparation, approval and dispatch of customer notifications relating to critical events and planned maintenance activity, working closely with local teams and senior management to help ensure correct and appropriate communication with customers

Customers may request the arrangement of activities, such as deliveries, collections, access and 'Remote Hands and Eyes' arising either from the Customer Portal or by e-mail.

In addition to being the single point of contact for customers, the ECSC is the knowledge hub for Interxion's European Data Centres. It helps Interxion to optimise service and to track and improve customer focus.

Key aspects of the ECSC are:

- Single-point-of-contact, pan-European service and operational helpdesk,
- ISO 27001 accreditations,

- ITILv3-trained staff (to a minimum foundation level),
- One contract, one set of service levels across all markets,
- 24x365 remote monitoring (critical alarms only), coordination and management,
- Coordination and dispatching of customer notifications for critical incidents and planned maintenance activity
- Service Level Agreement (SLA) based ticketing process, from ticket allocation to resolution (incident identification, escalation, management and resolution), and
- Multilingual capability.

3.1.3.4 Digital Technology & Engineering Group (DT&EG)

The Digital Technology & Engineering Group (DT&EG) team have facility experts located in Amsterdam. The team establishes the current and long-term direction of data centre standards to help keep Interxion data centres secure, highly reliable, competitive, green and energy efficient. DT&EG provide the following services:

- Digital Technology (both Facility and IT Engineering).
- Engineering (both Facility and IT Engineering).
- Data Centres Construction Projects (new build, expansion etc.) - control, support and reporting.
- Digital / IT Engineering Projects – planning, management and implementation.
- Energy Saving - planning, setting of targets, monitoring and reporting.
- Technical Data Centre Performance - advice, guidance, direction and authorization to carry out major changes, plans and procedures.
- Key Performance Indicators - controlling and reporting.
- Various Site Supports including training programs related to Key Performance Indicators (KPIs), Power, Cooling, Energy Saving, Security, Reporting, Crisis and Change Management and Management and Operations (M+O).
- Provide on-site training support related to new employees at key positions.
- Create and execute Interxion Data Centres Audit Programs related to security, operational performance and technical level of country organisation including quality, compliance and M+O matters.

3.1.4 Scope of the report

This document was prepared in accordance with the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC2). The scope of the report includes the cloud and carrier colocation data centre services and the Trust Services Principles (hereafter TSP) Availability and Security set forth in the American Institute of Certified Public Accountants (AICPA) section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. The scope of this report applies to the CPH1+2 and CPH-RS locations in Denmark, and the ECSC, HQ HR, HQ ICT and DT&EG functions based in the United Kingdom and the Netherlands.

3.1.5 External Subservice Organizations

There are no external subservice organizations with impact on the control environment of Interxion.

3.1.6 Changes to the Control Environment

CPH2 has been commissioned on April 15, 2016. No other significant changes to the control environment have occurred during the examination period. The Admin Software Panasonic system was decommissioned on August 1, 2016. Minor changes have been made to the controls in order to align the controls with the updated TSP section 100, *Trust Services Principles and Criteria, for Security,*

Availability, Processing Integrity, Confidentiality, and Privacy, effective for periods ending on or after December 15, 2016.

3.2 Components of the system providing the defined service

3.2.1 Infrastructure

CPH1+2 and CPH-RS customers can rent rooms, cages and rack space from Interxion Denmark ApS. Customers may only access their own space, which is controlled with card access readers and cameras and other methods determined by customers.

The CPH1+2 and CPH-RS data centres are equipped with Uninterrupted Power Supply (UPS), fire detection and suppression systems, backup generators, and Heating, Ventilating, and Air-conditioning (HVAC) systems to help protect from environmental attacks. The facilities offer redundant (N+1) UPS power and redundant (N+1) cooling as well as alarm and monitoring systems. The CPH1+2 and CPH-RS data centres support high-density power configurations and have been designed using Interxion's energy-efficient modular architecture, including free cooling and maximum efficiency components.

3.2.2 Software

Interxion Denmark ApS uses Sage Customer Relationship Management (hereafter CRM) and the Customer Portal to manage customer requests, including requests for access, deliveries, removals, 'Remote Hands and Eyes', customer queries, complaints, quote requests and incident management. SharePoint is used to manage change management requests and problem management. Critical equipment is monitored by the ECSC and Interxion Denmark by the use of the software tools. Customers can also use the Customer Portal to update access rights for their rooms, cages and rack space. ICT uses TOPdesk to manage service requests.

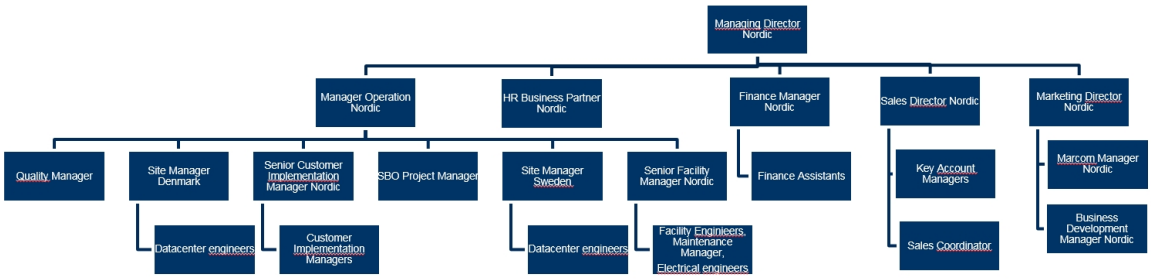
Interxion uses several types of software (on country level) to support their service provisioning. Whilst there is some regional variation, the systems in scope of the SOC 2 audit are: Building Control, Badge Access Control, Climate, Environmental Monitoring, Service Management / Maintenance, Fire Detection and Fire Suppression systems. In addition to this general statement, for clarity regarding Interxion Denmark ApS the following systems are in scope:

Software	Functionality
Avigilon	CCTV System
Alliance	Badge Access and Security Monitoring
L1 Identity Secure Admin / TBS Enrol Client	Biometric Finger Scanner Software
Admin Software Panasonic	Biometric Iris Scanner Software
Desigo Siemens, Netbotz	Climate and SLA Monitoring
(ION) / PMA Enterprice	Power Monitoring
DCIM / Iconics	Data Centre Monitoring System
Ultimo	Maintenance Planning System

Software	Functionality
Netbotz / Centre Scape	Environmental Monitoring System

3.2.3 People

Interxion Denmark ApS has a dedicated team assigned to the Operations for Customers Services and Infrastructure Management. In the Denmark headquarters, local teams support business and operations with Sales, Finance, Marketing, Quality and Security and Human Resources departments. Please see below for a high level organisational chart.



The Interxion Nordic Operations team is organized with an Nordic Facility Group, a Nordic Customer Implementation Group, a Nordic Build Out Project Manager, a Nordic Quality Manager and local Site teams. Additionally security agents are present 24x365 on-site at CPH1+2.

3.2.4 Policies & Procedures

All Interxion employees should adhere to the Interxion global policies and procedures that define how services should be delivered. These policies are available on the Interxion intranet.

3.2.5 Data

Data, as defined for cloud and carrier neutral colocation data centre services, constitutes account setup information. Account setup is processed online and provisioned through CRM by the ECSC. Other data excluded from the scope of this report includes data, applications and hardware installed by Data Centre customers.

3.3 Internal control environment

This section provides information about the five interrelated components of internal control at Interxion:

- *Control Environment* – sets the tone of Interxion, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- *Control Activities* – are the policies and procedures that help make sure that management's directives are carried out.
- *Information and Communication* – are systems, both automated and manual, that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- *Monitoring* – is a process that assesses the quality of internal control performance over time.
- *Risk Assessment* – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

3.3.1 Control environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The objectives of an internal control structure are to provide reasonable, but not absolute assurance as to the integrity and reliability of the organisation, and ensures the protection of assets from unauthorized use or disposition. Interxion Management has established and maintains an internal control structure that monitors compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values and competence of Interxion's employees, the policies and procedures, the risk management process and monitoring and the roles of significant control groups. The internal control structure is established and refreshed based on Interxion's assessment of risk facing the organization.

3.3.1.1 Organisational Structure

Interxion has a one-tier management structure with one board of directors, currently consisting of one Executive Director and six Non-Executive Directors. The board is responsible for the overall conduct of the business and has the powers, authorities and duties vested in it by and pursuant to the relevant laws of the Netherlands and the Articles of Association. In all its dealings, the board shall be guided by the interests of the Interxion group as a whole, including the shareholders and other stakeholders. The board has the final responsibility for the management, direction and performance of the Interxion group. The Executive Director is responsible for the day-to-day management of Interxion. The Non-Executive Directors supervise the Executive Director and the general affairs, and provide general advice to the Executive Director.

The Chief Executive Officer ("CEO"), the Executive Director, is the general manager of the business, subject to the control of the board, and is entrusted with all of the board's powers, authorities and discretions (including the power to sub-delegate) delegated by the full board from time to time by a resolution of the board. Matters expressly delegated to the CEO are validly resolved upon by the CEO and no further resolutions, approvals or other involvement of the board is required. The board may also delegate authorities to its committees. Upon any such delegation the board supervises the execution of its responsibilities by the CEO and/or the board committees. The board remains ultimately responsible for the fulfilment of its duties. Moreover, its members remain accountable for the actions and decision of the board and have ultimately responsibility for the Interxion's management and the external reporting. The board's members are accountable to the shareholders of Interxion at its Annual General Meeting of shareholders.

3.3.1.2 Integrity and ethical values

Interxion has the ambition to be an industry-leading provider of carrier neutral internet data centre services. In order to pursue this ambition, it depends on its highly motivated, committed and skilled people. People who set ever higher standards when it comes to addressing the challenges of Interxion's industry, but also when it comes to acting in accordance with high ethical standards. It is a core value of Interxion and one of the drivers for its future that it has and will remains true to its ethical principles, irrespective of how hard Interxion competes and strives to improve the business.

As a public company, Interxion is required to have a formal set of guidelines that explains the ethical principles that Interxion will follow as it conducts business. This is contained within the CoC and sets out the principles that Interxion, as a company, and as individuals will adhere to. The CoC also helps the Interxion employees to understand the responsibilities as employees of the Interxion group of companies. To that end, the CoC contains guidelines and information on how Interxion should behave but also what Interxion should do when unacceptable behaviour has been identified.

3.3.1.3 Governance and Oversight

Interxion has a comprehensive governance and oversight framework it applies itself to a strictly enforced audit and governance framework. It complies with Sarbanes-Oxley Act (SOx) Section 404 and has a comprehensive ISO (International Organization for Standardization (ISO) / IEC (International Electrotechnical Commission) accreditation in Information Security and Business Continuity. This is, by the nature of its business, essential. This is backed by oversight from board level. All resolutions of the board are adopted by a simple majority of votes cast in a meeting at which at least the majority of the Directors are present or represented. A member of the board may authorise another member of the Board to represent him/her at the board meeting and vote on his/her behalf. Each Director is entitled to one vote (provided that, for the avoidance of doubt, a member representing one or more absent members of the board by written power of attorney will be entitled to cast the vote of each such absent member). If there is a tie, the Chairman has the casting vote.

The board meets as often as it deems necessary or appropriate or upon the request of any member of the board. The board has adopted rules, which contain additional requirements for Interxion's decision-making process, the convening of meetings and, through separate resolution by the board, details on the assignment of duties and a division of responsibilities between Executive Directors and Non-Executive Directors. The board has appointed one of the Directors as Chairman and one of the Directors as Vice-Chairman of the Board. The board is further assisted by a Corporate Secretary. The Corporate Secretary may be a member of the board or a member of the Senior Management team and is appointed by the board.

3.3.2 Control activities

This table summarizes the mapping of the common criteria (section IV) and the control activities (paragraph 3.3.2).

Criteria categories / Paragraphs within 3.3.2	Additional criteria for Availability	CC1.0: Organisation and Management	CC2.0: Communications	CC3.0: Risk Management and Design and Implementation of Controls	CC4.0: Monitoring of Controls	CC5.0: Logical and physical access controls	CC6.0: System Operations	CC7.0: Change Management
3.3.2.1: Policies and procedures	ü	ü	ü	ü	ü	ü	ü	ü
3.3.2.2: Risk Assessment and Security Management	ü	ü	ü	ü	ü	ü	ü	ü
3.3.2.3: Personnel Security				ü		ü	ü	
3.3.2.4: Logical Access	ü	ü	ü	ü	ü	ü	ü	ü
3.3.2.5: Physical Security	ü			ü		ü	ü	
3.3.2.6: Environmental systems	ü			ü			ü	
3.3.2.7 Monitoring and reporting	ü	ü	ü	ü	ü	ü	ü	ü
3.3.2.8 Preventive Maintenance	ü	ü	ü				ü	ü
3.3.2.9: Incident Management	ü	ü		ü		ü	ü	
3.3.2.10: Problem Management	ü	ü		ü		ü	ü	
3.3.2.11: Change Management and Maintenance	ü	ü	ü	ü		ü	ü	ü
3.3.2.12: Communications	ü	ü	ü	ü			ü	
3.3.2.13: Business Continuity	ü	ü	ü	ü		ü	ü	ü

3.3.2.1 Policies and procedures

Policies and procedures supporting the cloud and carrier neutral colocation data centre services covered by this system description are created and held in HQ based “Tier 1” policies and procedures mandated by the Information Security Committee and are almost exclusively owned and signed off by the Vice President Operations. The only exception to this is documents that are technical in nature or procedurally complex enough to warrant ownership by a Subject Matter Expert. Where this is the case it is noted within the document or those owned and managed by HQ HR. These documents are to be reviewed at country level to ensure all entities are fully aware of them and understand them.

All Tier 1 documents are reviewed regularly (at least annually) by the HQ Senior manager Quality and Compliance. For the local policies and procedures (Tier 2 and 3) it is expected that these are regularly reviewed by the local owner. It is also implicit that these are reviewed during the various internal audits carried out by both technical (DT&EG) and compliance (HQ Senior Quality and Compliance Manager)

The below is a comprehensive list of central and local policies and procedures covered by this system description and inherent in Interxion’s compliance with its TSP’s. Additionally the Information Security Management System (ISMS) Information Security library has been updated to the latest ISO27001:2013 standard from the 2005 version.

Document name	Mandate	Country	Type
Risk Management Framework	HQ	Global	Policy
Interxion Information Security Policy	HQ	Global	Policy
Acceptable Usage Policy (AUP)	HQ	Global	Policy
Personnel Screening Policy	HQ	Global	Policy
Physical Access Security Policy	HQ	Global	Policy
Policy Against Malicious Code (malware)	HQ	Global	Policy
Access Control Policy	HQ	Global	Policy
Interxion Information Security Compliance Policy	HQ	Global	Policy
Data Protection & Privacy Policy Statement	HQ	Global	Policy
Risk Assessment Procedure	HQ	Global	Procedure
Confidentiality Agreements	HQ	Global	Procedure
External Parties: Information Security Procedure	HQ	Global	Procedure
Inventory & Ownership of Assets	HQ	Global	Procedure
Versioning & Classification	HQ	Global	Procedure
Reporting physical and environmental Security Weaknesses & Events	HQ	Global	Procedure
Documented IT working procedures	HQ	Global	Procedure
Change Management Process and Procedures	HQ	Global	Procedure
System Planning & Acceptance	HQ	Global	Procedure
Backup Procedures	HQ	Global	Procedure
Network Controls & Services	HQ	Global	Procedure
Media and Information Handling Procedure	HQ	Global	Procedure
Business Information Systems	HQ	Global	Procedure
Access Control Rules & Rights for Users/User Groups	HQ	Global	Procedure
Joiner & Leavers Procedure	HQ	Global	Procedure
Remote Access Procedure	HQ	Global	Procedure
Control of Operational Software	HQ	Global	Procedure
Vulnerability Management	HQ	Global	Procedure
Reporting Information Security Weaknesses & Events	HQ	Global	Procedure
Business Continuity Planning	HQ	Global	Procedure
Testing, Maintaining & Re-assessing BC Plans	HQ	Global	Procedure
Crisis Management Process and Procedures	HQ	Global	Procedure
Incident Management Processes and Procedures	HQ	Global	Procedure
Business Continuity Plan	CPH1+2, CPH-RS	Nordic	Procedure
Disaster Recovery Plan	CPH1+2, CPH-RS	Denmark	Procedure
Crisis Resolution Steps part 2 Building	CPH1+2, CPH-RS	Denmark	Record
Crisis Resolution Steps part 2 Chilled Water	CPH1+2, CPH-RS	Denmark	Record

Document name	Mandate	Country	Type
Crisis Resolution Steps part 2 Power	CPH1+2, CPH-RS	Denmark	Record
Evacuation plan	CPH1+2, CPH-RS	Denmark	Procedure
Staff Introduction during crisis	CPH1+2, CPH-RS	Nordic	Procedure
Local Significant Incident Routine	CPH1+2, CPH-RS	Nordic	Procedure
Nordic BCP test plan OPS training	CPH1+2, CPH-RS	Nordic	Record
Badge Access Security monitoring platform	CPH1+2, CPH-RS	Denmark	Procedure
Biometric Finger scanner Platform	CPH1+2, CPH-RS	Denmark	Procedure
CCTV Platform Description	CPH1+2, CPH-RS	Denmark	Procedure
Cooling Monitoring Platform Description	CPH1+2, CPH-RS	Denmark	Procedure
Power Monitoring Platform	CPH1+2, CPH-RS	Nordic	Procedure
Maintenance planning platform system	CPH1+2, CPH-RS	Nordic	Procedure
Energy billing platform system	CPH1+2, CPH-RS	Nordic	Procedure
Datacentre platform monitoring system	CPH1+2, CPH-RS	Nordic	Procedure
Training	CPH1+2, CPH-RS	Nordic	Procedure
Training and Certificate	CPH1+2, CPH-RS	Denmark	Record
ISO Document Denmark 2016	CPH1+2, CPH-RS	Denmark	Record
Local Significant Incident Routine	CPH1+2, CPH-RS	Denmark	Procedure
Local Application Users	CPH1+2, CPH-RS	Nordic	Procedure
Physical Site Security Audit	CPH1+2, CPH-RS	Nordic	Procedure
Environmental Risk Summary	CPH1+2, CPH-RS	Nordic	Procedure
Self-Assessment	CPH1+2, CPH-RS	Nordic	Procedure
House rules	CPH1+2, CPH-RS	Denmark	Procedure
Security Alarm handling responsibility and documentation	CPH1+2, CPH-RS	Nordic	Procedure
Infrastructure Alarm handling responsibility and documentation	CPH1+2, CPH-RS	Denmark	Procedure
Access Rights and Access Card Handout	CPH1+2, CPH-RS	Nordic	Procedure
Building Security	CPH1+2, CPH-RS	Denmark	Procedure

3.3.2.2 Risk Assessment and Security Management

The Interxion senior management team has assigned lead responsibility for information security to the Vice President (VP) Operations Support of Interxion. In this description, security is mainly focused on physical and environmental security (i.e. limited to those policies and controls that may impact customer information security).

Interxion maintains an Information Security Management System (ISMS) which details policies and controls that help determine the Interxion Information Security effectiveness. In particular, the ISMS is defined as the part of Interxion Denmark ApS overall management system which, based on a business risk approach, enables management to establish, implement, operate, monitor, review, maintain and improve information security within Interxion Denmark ApS. The ISMS, and thereby the organisation of Information Security, is designed to meet the criteria and requirements of the risk management framework, to take into account the risk acceptance criteria and current legal, regulatory and contractual requirements.

Within the local entities the Managing Director carries full responsibility for aspects of ISMS, including asset management and implementation of ISMS requirements, as well as local operating procedures and work instructions that are required to comply with the ISMS. Interxion Denmark ApS has its own Site Manager in charge of managing the security teams of the buildings, including trainings and controls. Line Management is responsible for ensuring employees of Interxion and where relevant, contractors and third party users state their understanding of their responsibility for information security in their employment or service contract and receive appropriate awareness training and regular updates in organizational policies and procedures that are relevant for their job or role function.

Line Management will comply with all policies and procedures that Interxion has in place to secure its systems services and business at all times. Periodic meetings are held between Line Management, ECSC and its relevant stakeholders to discuss security and availability. These meetings due to the operational nature of the teams involved are frequent though not always formal. Quick discussions and decisions are needed. In all matters where security is concerned the ECSC direct notifies the relevant parties of any items that need escalation prior to agreement. The same is true of the ICT function. Due to the high level of complexity in the ICT systems and services ICT is in the process of moving from physical systems to a more easily understood (from the internal and external clients perspective) service based model. When moving towards a Service Oriented Model, this will also align with the changes in the standards Interxion complies with.

3.3.2.3 Personnel Security

Responsibilities for specific information security procedures are defined and documented in individual job descriptions. Staff (and certain third party contractors where required) have accepted their specific responsibilities as detailed in the Acceptable Use Policy (AUP) for which the individual is required to acknowledge acceptance before they are authorized to access organisational information assets.

Employee background checks are conducted for Security Guards and other employees based on the level of employment. Interxion requests an official clearance certificate for employees, and for Security Guards and Operational personnel, an additional criminal background investigation is required. Please note where local privacy and data protection laws prohibit this all reasonable efforts are carried out to comply with this procedure, however the local entities country laws are respected as precedent.

A Security Awareness Program has been implemented for employees to support organisational security policies during the course of their work. Employees found to be in violation of Interxion Security policies are subject to disciplinary action up to and including termination of employment. Employees are required to report security incidents and weaknesses.

3.3.2.4 Logical Access

In the case of logical access to internal ICT systems all requests for access are managed by logging of a request in TOPdesk (HQ systems) or by a local authorization access request form (local ICT systems). If a user requires access to Data, an ICT system or Service it must then be logged and where applicable signed off by the users' line management. Where appropriate and possible Interxion ensures all the systems in scope are managed with passwords and user ID submission. The Access Control Rules & Rights for Users/User Groups procedure supplies control for this. Users have a unique user ID for their personal and sole use (where possible).

If applications do not have a unique user ID for each user and require the use of generic accounts, additional security measures are implemented to restrict the access to appropriate personnel. The Quality Manager is responsible for conducting a regular (at least quarterly) review on access to all generic accounts. The use of the generic accounts is limited by restricting the access to the password of the generic accounts which is only accessible for authorized personnel. Personnel with access to the generic accounts are included in an exception form, which is used to determine that the generic account access is still restricted to appropriate personnel. Password authentication is for internal systems via the Active Directory account. For other systems identified for use appropriate controls are applied. All formal access requests are logged as a ticket in TOPdesk (HQ access) or as a local authorization access request form (local ICT systems) and must be authorised by a line manager. There are formal user registration and de-registration procedures (Access Control Rules & Rights for Users/User Groups procedure, Joiner & Leavers procedure and the Remote Access procedure) for granting and revoking access to all information systems and services.

Access to logical assets and ICT systems is via logging a TOPdesk ticket (HQ systems) or by a local authorization access request form (local ICT systems). Regular reviews are carried out of account activity and those users that HQ HR has notified HQ ICT, Local ICT and the ECSC of leaving. Local entities will also follow the controls laid out in the Information Security Manual. HQ HR operates a policy of standard roles. These roles are applied to all incoming employees. This list of roles has inferred access limitations based on Department need and where applicable seniority.

Interxion maintains a tiered approach to its logical security. Where possible all networks are physically kept separate. Where this is not possible or practical every care is taken to minimise the physical interconnections between them. In the case of data centre\management networks this is mandatory. Interxion maintains a strict policy of Change Management on both its Corporate and data centre environments. Any changes to the Corporate or data centre management must be approved by the Change Advisory Board.

Interxion maintains an up to date firewall complex to maintain its central security. Individual entities will have central data and access protected by this same system. Additionally there is a live intrusion prevention system in place to maintain central control of risk.

All users must both sign the AUP and also ensures its employee have also read and signed up to the Media and Information Handling Procedure. All users must adhere to the Information Security Policy.

TOPdesk tickets and CRM tickets are actively reviewed to ensure security and availability breaches are both captured and investigated. The Risk Assessment process is used to ensure any event that is likely to impact the Business Continuity Plan is identified and mitigated.

3.3.2.5 Physical Security

Interxion uses security perimeters to protect areas that contain information and information processing facilities. Secure areas are protected by appropriate entry controls to help ensure that only authorized

personnel are granted access. Interxion has a comprehensive physical security program, which operates in a continuous improvement mode. Wherever possible, the security controls adopted utilize a layered approach at each location in which the controls become more stringent from the outermost perimeter of the facility to the interior restricted spaces.

The CPH1+2 and CPH-RS colocation data centres physical security controls are designed as a "building within a building" and include:

- The data centres CPH1+2 are permanently secured by security guards that are present 24x365 on site. In both CPH1+2 and CPH-RS guards patrol inside and outside of the data centres.
- Data Centre perimeter is protected by Closed-Circuit Television (CCTV) monitored 24x365 by the security guard. A 24x365 CCTV (external and internal) system directly monitored by the Security office. The CCTV footages are stored for 30 days
- Access control system records any entries or exits in the building, private rooms and other private spaces
- Equipment to prevent unauthorized access to customer equipment:
    - Fingerprint readers are used to permit entry into the building
    - Proximity cards, typically combined with biometric readers
    - Mantraps Burglar alarm systems

Interxion provides additional levels of security for customer cages and cabinets depending on customer requirements (i.e. badge system, biometric readers at an entrance, video camera, etc.). Interxion buildings are supervised by on-site security personnel, as well as the ECSC 24x365.

Customer authorised persons with permanent access permission may access their equipment, while persons with intermittent authorization have to register in advance. Customers decide if they would like to permit access to their own staff and service providers

Visitors must provide proof of identity by national ID or Passport and this is checked against predefined authorization access lists. Visitors are logged, monitored by video surveillance cameras and must have a personal access card, unless escorted by Interxion security personnel. Badges must be worn and clearly visible, and visitors must identify themselves to Interxion security personnel when requested to do so.

Interxion's employee and contractor physical access to the Interxion facilities, data centres, and Interxion areas within colocation data centres is limited to authorized personnel and is based on job function. The Managing Director is responsible for authorizing access to Interxion areas, and security levels and access are reviewed on a periodic basis. All permanent physical access rights are requested using a central process managed by ECSC. Access is validated by an ECSC agent before access is granted (unless the customer uses the portal).

3.3.2.6 **Environmental systems**

a) Power Supply

Interxion has taken extensive measures to equip the premises with a reliable and resilient power infrastructure, including dual energy access points to the facility, diesel generators with sufficient fuel storage, UPS systems and various redundant elements in the distribution network throughout the premise.

b) Fire Protection

The premises are equipped with fire retardant walls, optical and thermal smoke detectors (underneath and above the flooring) and direct lines to fire stations. Additionally, the customer space is secured by automatic gas-based fire suppression systems as a first line of defence against fire. The premises are also equipped with hand held fire extinguishing systems.

For additional protection from fire, Interxion operates Very Early Smoke Detection Alarm (VESDA) systems. In case of smoke, this system immediately alerts Interxion staff allowing them to take appropriate action before a fire starts.

c) Water Detection

Interxion facilities include water detection systems installed in areas that may be susceptible to leakage. The water detection alarms are relayed directly to the ECSC, as well as to the relevant local security and engineering.

d) Climate Control

For optimum performance, equipment is maintained and continuously monitored in a climate-controlled environment. The average room temperature and humidity level is controlled at a suitable level. Multiple air conditioning units provide redundant capacity. Down-flow cooling units help ensure maximum cooling of equipment.

3.3.2.7 Monitoring and reporting

Interxion buildings are supervised by on-site security personnel, as well as the ECSC 24x365. Moreover, critical alarms raised on the Building Management System (BMS) are monitored 24x365 in the data centre at the security office by the security guard, at the ECSC and by the on duty and on call engineers.

The capacity of Interxion's systems is not a flat structure. Client and data centre capacity is captured and analysed through the various power and systems reports. This is not specific, as there are many different ways that metrics have grown over time primarily due to the client's needs. Typically, clients (where contractually stipulated) receive a monthly service report. This again typically gives both operational support data and service delivery information.

Interxion ICT infrastructure is managed with a policy that works on a 'just in time' principle. This is both for efficiency but also to ensure that resources whilst never maxed out are run to their optimal potential. There are monthly meetings at operations level to communicate current capacity and provide a framework for the business to inform ICT proactively of requirements rather than waiting and dealing with each new request as an incident. Additionally meetings are held periodically and as required to ensure capacity is at a level which fully supports both its business and client requirements.

Where contractually agreed, Interxion will provide regular reports to customers. The scope, content and period of this reporting is agreed contractually at the earliest stage possible within the implementation project.

These reports could include the following items:

- An access log of the physical access to the customer rooms. The provision of reports on exits requires that the customer orders an optional service to allow the installation of badge readers that permit the exit of authorised visitors from the customer rooms;
- Key performance indicators (by room / cage / space):
    - Power availability rate;
    - Temperature;
    - Humidity;

- Monitoring of the actual power consumption of the customer's equipment. The monitoring is expressed as a percentage of use compared to the contractual commitment (by room / cage / space);
- Log of the 'Hands and Eyes' interventions and infrastructure events (incidents / maintenance/changes);

The DT&EG department prepares KPI's:

- Square metres (SQM): Monthly corporate square meter reports;
- Energy: Monthly corporate energy usage reports;

There is a standard process ('Reporting Physical & Environmental Security Weaknesses & Events') for reporting security breaches. All personnel are required to follow this procedure for reporting physical and environmental security weaknesses or events.

The Manager Operations is responsible for managing security responses and pending on severity of the impact, escalate to the Managing Director of the local entity and the VP Operations Support of Interxion.

Physical and environmental security weaknesses and events are reported, immediately as they are seen or experienced, via email or phone to the local nominated Security Manager.

Events will be assessed, classified and an appropriate response will be initiated. We will use the following classification for security events:

- **Events impacting only local standard operational processes and procedures.**

The responsibility for managing these events is with local management and does not need external reporting.

However it will still be required for the local Manager Operations to ensure that involved personnel are made aware on the incurred breach and remind involved personnel of the local laws and regulations and related disciplinary procedures.

- **Events on a local scale impacting customer security.**

If there is a disturbance of customer assets or a breach of customer security this should be reported to the Manager Operations, who will inform the ECSC in accordance with the Major Incident & Crisis Procedure. Where customers have assigned a Security contact the incidents shall be reported by the Manager Operations to the customer Security contact.

- **Events resulting from malicious intent of persons (violation of rules, deliberate attempts to breach security processes, theft).**

The events should be reported to the Managing Director and Interxion VP Operations Support and handled in accordance with disciplinary procedures and local laws and regulations shall be reported by the Manager Operations to the customer Security contact.

- **Events threatening Physical Security perimeters and Access Control systems and procedures.**

The events should be reported by the Manager Operations to the Interxion Director of Engineering and Interxion VP Operations Support.

- **Events indicating existence of an external threat to Interxion premises, staff and continuity.**

The Manager Operations is responsible for updating and reviewing the local Risk Analysis process and informing the Managing Director of the local entity and the Interxion VP Operations Support.

Local management are required to ensure that all personnel attending the premises are trained sufficiently to understand the rules and regulations and how to act on a physical / environmental incident.

All escalations of incidents are logged by email. The local Manager Operations (MO) is required to retain a Security event log documenting all events and corrective actions and conclusions. Breaches are typically discussed at MO level in the MO meetings held biweekly. If a major incident is found

(via the problem management process) to have an impact on their sites these sites will be informed as a matter of course.

3.3.2.8 Preventive maintenance

Preventative maintenance is conducted to help provide continued operation of the data centre and is performed per schedules provided to customers by Interxion, including vendors of the data centre equipment. Preventative maintenance procedures for data centre equipment are documented, detailing the procedure and frequency of performance in accordance with internal or the manufacturer's specifications and regulatory control of Interxion's facilities (according to the local regulations e.g. electrical). Interxion maintains a schedule of planned and actual service dates, and retains copies of the service reports, together with fault reports and details of preventative or corrective actions.

3.3.2.9 Incident Management

Incidents are detected either from staff on site or from the ECSC. They are logged in CRM and escalated to the staff on site. There is an incident coordinator both on site and at the ECSC, communicating on the progress to resolution so that the ECSC can inform customers accordingly.

During an outage, communication is also established via a conference bridge with the customer and key people on site, usually the Manager Operation, the Facility Manager, the Site Manager and a DT&EG engineer. A root cause analysis is provided for any customer impacting incident

If the customer needs to escalate an issue, a ticket is logged with the ECSC. The ECSC will follow the documented procedure for escalation and contact the Manager Operation and the Managing Director. Depending on the severity of the incident, the issue could be escalated to members of the HQ Management team.

A Crisis Management procedure defines the Incident and crisis Management on Interxion Site Infrastructure. An Incident is defined as any interruption or degradation of quality of a service (linked to the site infrastructure) that was not planned. Incident Management aims at re-establishing the service as fast as possible and to manage internal and external communication. The Crisis Management procedure aims at managing resources and the communication of incidents impacting customers with a threat to risk a complete rupture of service.

ECSC provides a knowledge management hub for incident identification, escalation, management and resolution.

3.3.2.10 Problem Management

Alarms and incidents are analysed thoroughly and corrective actions are achieved via the problem management process. A maintenance window is scheduled to apply any such changes.

Interxion also works closely with its suppliers of critical equipment using tools such as root cause analysis, to understand a failure and help prevent it from recurring.

3.3.2.11 Change Management and Maintenance

Changes to the service production system are subject to the formal change management process. Changes are implemented during ongoing service delivery to Interxion's customers within the data centres infrastructure, and should have no impact. The change management process follows a structured approach and includes notification to involved parties. The change management procedure is documented and stored in the Field Operations Manual and linked within the ISMS.

All changes are reviewed both technically and by the Change Advisory Board prior to approval. Changes are also approved by the Change Advisory Board (Senior Management). This is to ensure they have been evaluated to determine the potential impact upon both availability and security. This process includes understanding the 'Area of Impact' of the change by determining which stakeholders (be they clients or otherwise) are affected. Ongoing risk assessment is carried out both at the operational level and also for budgetary planning. The scope of this includes infrastructure, data considerations, software and the effect of changes upon support and delivery policies and procedures.

It must also be noted that Interxion also integrates it change process with incident management. 'High Severity' incidents can have emergency changes raised against them based upon a standard impact x urgency assessment. The subsequent priority given to processing a change assists in scheduling of reactive emergency changes where significant impact or risks are perceived based upon security, availability and capacity considerations. Customers are notified of changes that have potential customer impact. All changes to data centre infrastructure (including monitoring systems) are under the mandate of change management. The high level steps for change management are:

- Step 1: Initiate change request;
- Step 2: Review and approve change request through the change board;
- Step 3: Notify stakeholders of pending change;
- Step 4: Implementation of the change;
- Step 5: Notify stakeholders of completion of change.

Notifications are sent in advance for maintenance that may have a risk of impact to customer operations. This gives customers the opportunity to review and raise any concerns to Interxion before changes are implemented.

3.3.2.12 Communications

Once a new contract is signed, the customer account is created in the relevant Sales Management Software and CRM (please note at this stage also the Service Level Agreement, which includes Interxion's responsibilities, is communicated to customers upon signing the initial contract) . The ECSC then sends a standard introductory 'Welcome Pack' to the customer, which includes:

- Interxion contact details;
- Raising issues with Interxion;
- Escalation process;
- Access procedure and the related lists where requested;
- Procedures on the delivery / removal and installation of equipment;
- Hands & eyes procedures;
- Notification process for maintenance;
- Emergency and escalation\ maintenance contacts.

When customers take up occupation of space within an Interxion facility, customers are asked to follow a set of "House Rules" within Interxion facilities.

3.3.2.13 Business Continuity

Interxion is certified according to Standard ISO 22301 Business Continuity Management which was developed to minimise the risks of disruptions that can impact a business. This means that Interxion has adopted a uniform process to Business Continuity Management for the development and maintenance of business continuity throughout the data centre. It addresses the information security requirements needed for the Interxion's business continuity and help ensure that data centre solutions can meet the specific customer needs agreed upon in customer contracts and service level agreements.

The Business Continuity Plan includes an overview of disaster recovery preparation plans for the technical infrastructure in accordance with customer needs. The critical processes are identified in the plan, together with the responsibilities for restoration of service in the event of a loss of continuity. The Business Continuity Plan includes a standard alert, escalation and plan invocation procedure. The Business Continuity Plan is maintained and subject to yearly testing, maintenance and improvement.

At a lower level full daily backups are taken of system critical data. All the organization's information assets are subject to backup requirements, excluding PDAs, mobile phones, notebook computers and desktop computers. All owners of information assets are required to ensure that backup arrangements and Operations Work Instructions that conform to the requirements of this procedure exist for each of the assets for which they are the identified owner. The ICT Manager is responsible for ensuring that IT staff executes the identified backup for central systems as required and for identifying and reporting any faults, failures or errors. The ICT Manager is responsible for documenting, testing and maintaining the restoration process in line with business needs.

- All production servers are backed up daily.
- All backups have the following retention scheme:
    - 1 week backup is available on a daily basis.
    - 1 month backup is available on a weekly basis
    - 1 year backup is available on a monthly basis
    - 7 year backup is available on a yearly basis
- All backups are monitored on a daily basis and restores are tested every 2 months.

3.3.3 Information and Communication

Interxion

Regular operational Meetings are held with site personnel to update them on scheduled customer activities (i.e. new customers, installation in progress), infrastructure and facilities activities (e.g. preventive\corrective maintenance and major changes) and general information on people, organisation, trainings, projects and actions plans.

A monthly call between the Manager Operations and the ECSC Manager is held, to align activities and administrative aspects, including major events.

In each department, periodic meetings are held within Interxion HQ and also the countries to align strategy, analyse data, and act on common action plans, software deployment and improvements. A local management committee is also sits regularly to share information in the departments. Regular management reviews are drawn up in order to evaluate Management System efficiency and performance.

Interxion communicates regularly with all resources regarding training, new management system documentation published on the intranet (i.e. policy, manual, procedure and instruction) or posted onsite, emails, conference calls, and specific events for employees. Personnel also participate in workgroups for operational improvements.

Key maintenance suppliers (for cooling, UPS, diesel generators) are regularly called to periodic meetings to prepare scheduled maintenance operations or follow-up on agreed KPI's and to also agree and review improvement action plans.

Customers

Customers can interact with Interxion by following procedures and processes described in the Welcome Pack or use the Customer Portal for site-access requests, remote-hands and eyes intervention and complete tasks related to their installations at Interxion data centres.

Customers are systematically informed of maintenance activities and all relevant operational activities that have been assessed for impact to them. Where possible proactive maintenance activity is scheduled annually and the affected customers are notified by the ECSC.

In cases where an unforeseen event occurs such as an incident or the resulting need for an emergency change, the ECSC communicates the progress to resolution and informs customers accordingly, the period of this update is based on the estimated time to fix. During an outage, communication is also established via a conference bridge with the customer and key people on site at the data centre.

Interxion Denmark ApS can provide reports to customers and hold regular meetings with customers as a contractual option. For some of the larger, multi-site customers, Interxion has a dedicated team conducting service reviews and preparing monthly or quarterly reports. These teams will fulfil contractual obligations regarding reports and customer meetings independent of the operations teams but all relevant data and information is shared via the aforementioned communications processes and mediums.

3.3.4 **Monitoring**

Interxion has clearly defined processes in place to monitor the services provided to customers and its internal controls. Interxion buildings are supervised by on-site security personnel, as well as the ECSC 24x365. In terms of assessing the effectiveness of the controls Interxion periodically performs internal audits based around the concept of identifying risks that could inhibit the effectiveness of the controls. Where applicable metrics are generated periodically (where appropriate) from KPI's extracted from empirical data (such as the service management tools in use) to ensure that control processes are functioning as expected.

These audits are carried out at local level by the Interxion Senior Manager for Quality and Compliance. They focus (amongst other things) on all areas of physical security including security staff, procedural and policy awareness, the effectiveness of physical access controls (such as building access), Mantraps, CCTV camera effectiveness. These audits are committed to reducing the risk of physical security breaches and to minimise the vulnerabilities in Interxion's systems and services. Where vulnerabilities present a significant risk, treatment plans are put in place to mitigate them to an acceptable level. Risks are addressed and documented in the relevant local Operations Procedures and Work Instructions.

Local Self-Assessment via continuous random controls based on population to verify that the implemented controls are efficient and procedures are followed is implemented. Physical Site Security Audit is performed annually to verify the facilities; building, fence, security systems, CCTV, access etc.

An Information Security Committee is implemented, having regular meetings (quarterly as a minimum). Responsibilities are:

- Ensure compliance with Global procedures and ISO27001 / ISO22301
- Assessment of Security Breaches, initiate preventive actions where needed and relevant
- Assessment of Exceptions
- Coordination of Risk Assessment and Risk Treatment plan
- Ensure adequate training / Awareness related to Information Security and Business Continuity
- Local audit planning
- Self-Assessment
- Supplier Management Follow up

Network penetration testing is carried out by a trusted third party (SecureLabs) on an annual basis (usually in the first half of the year). Secure labs are comprised of senior security consultants and engineers are experts in the field of enterprise system security. They are certified by the Information Systems Security Certification Consortium (ISSC2) and the Certified Information System Security Professionals body (CISSP). This test includes penetration testing on the external Addresses that Interxion utilises. Its primary objective is to identify areas of increased risk in the external IT environment.

The focus of the penetration testing is:

- The profiling of information available which relates to the Interxion brand and how it could be misused by a malicious attacker
- Assessment of the infrastructure used to facilitate Interxion's services and applications
- Determination of visible systems (those potentially accessible from the internet)
- Determination of the services running on these systems
- Manipulation and penetration of the management interfaces
- Manipulation of the applications that run on the back end
- Manipulation and gathering of data. Directly from databases, by using application related hacking techniques such as enumeration of data

The primary focus is access control. Will a potential hacker succeed in:

- Gaining access to confidential, classified or secret information
- Bringing substantial financial impact and or reputational damage to Interxion
- Endangering the company continuity
- Creating a newsworthy incident
- Endangering the safety of visitors, employees or customers of Interxion

Vulnerability scans are performed as part of the yearly schedule of audits. The Senior Manager Quality and Compliance schedules internal audits; each internal audit is carried out according to the standard procedure. Vulnerabilities are consistently assessed with regularity via the Vulnerability Management procedure.

The identified asset manager of each operational system is responsible for monitoring vulnerabilities and vendors' releases of patches and fixes and installing operational software updates, patches and fixes on the operational systems, is also responsible for maintaining the test environment, testing operational software updates and new implementations.

- The ICT Manager is responsible for the operational (live) environment.
- The asset owners are responsible for tracking likely vulnerabilities in and patches available for their assets.
- Identified vulnerabilities for organizational assets are all judged as priority 1 and acted upon in a similar way.
- High value or high risk systems are treated ahead of other systems
- All vulnerabilities are judged as 1 classification and will first be assessed for seriousness and required controls (patching; turning off/removing services affected by the vulnerability; adapting or adding access controls; increased monitoring; awareness enhancement).
- The required controls will be actioned through the change management procedure
- Available patches must be risk assessed, taking into account the balance between risks in installing and not installing, before the final decision as to necessary controls can be made.
- External points of contacts are regularly assessed for risks and the firewall polices have been designed to mitigate any unauthorised access or intrusion to Interxion's systems, ICT services and Data. Our firewall system is annually tested in line with our external penetration testing In addition to this Interxion regularly tests its firewall and Intrusion prevention systems and procedures as part of our Business Continuity Testing.
- It is company policy that anti-virus software (OfficeScan) is installed on all Interxion workstations, laptops and servers that support this control system. All these Configuration Items are regularly reviewed to ensure they have the latest version of the anti-virus software

on them wherever possible. The software is periodically updated and a report is created for those systems which show up as not having been updated in the recent past.

Interxion is continuously improving the services provided to its customers (i.e. service quality, security of information, facilities). The following audits are regularly performed to help achieve this objective:

- Internal Operational audits: Facilities and systems preventive maintenance program, operating procedures, energy efficiency, knowledge of technical and procedural staff managing sites (Recurring)
- External audit: finance and accounting (Quarterly)
- Internal audit: finance and accounting (Annually)
- Internal audit ISO\IEC 27001 & ISO22301 (Annually)
- External audit: ISO\IEC 27001 & ISO22301 (per certification scheme)

3.3.5 Risk Assessment

Interxion performs risk management in accordance with requirements laid down in ISO\IEC 27001:2013 and 22301:2012, which promotes analysis and handling of business risks. This process is a critical component of Interxion's internal control system, as risk is interpreted by Interxion as conditions that may impact service delivery to customers and may potentially breach service level agreements.

The purpose of Interxion's risk assessment process is to identify, assess and manage risks that affect the organisation's ability to achieve its high security objectives. The process includes:

- Identification of potential risks, which affect the Physical Information Technology environment from an ICT perspective. This is done both from a technical and business point of view.
- Assessment of significance, probability and consequence of potential risks.
- Measures and controls that could be implemented to reduce the probability that risks occur in a cost effective way.

Risk assessment is a continuous process performed at least annually or following substantial changes to the risk profile. Interxion aims to quantify relevant risks in order to objectively decide on applicable controls and possible treatment of risk. Risk treatment plans are documented and a consolidated, corporate approach to risk treatment is adopted in order to implement the selected controls consistently amongst Interxion entities.

3.4 Criteria and Controls

The Trust Services Criteria and the controls that meet the criteria are listed in the accompanying '*Description of Criteria, Controls, Tests and Results of Tests*'.

3.5 Key User Responsibilities

Interxion has designed and implemented its controls to meet its commitments and requirements as it relates to the Trust Services principles of security and availability. Interxion has communicated to its user entities that they have certain key responsibilities for the performance of controls in the operation of the Cloud and Carrier Neutral Colocation Data Centre System provided by Interxion Denmark ApS in order for them to address the security and availability of their use of the system. The responsibilities presented below should not be regarded as a comprehensive list of all controls which should be employed by customers.

CC5.5: Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet Interxion's commitments and system requirements as they relate to security and availability.

Client management is responsible for:

- Ensuring that only authorized client personnel have access to the customer equipment and space of the client.
- Ensuring that access to customer equipment and space is restricted to authorized personnel via Access Control Lists (ACL) administered by the ECSC. These are procedurally integrated with each data centre Badge Management System. It is the client responsibility to maintain an accurate ACL for its equipment.
- Ensuring that, whilst the ECSC and Data Security staff periodically review access to CPH1+2 and CPH-RS, only authorized people (registered ID) are present on the ACL.
- Ensuring that access requests to CPH1+2 and CPH-RS are submitted to the ECSC in advance by authorized requestors only.
- Ensuring that changes to authorized requestors and approvers are communicated to the ECSC, however the preferred method is for clients to manage their own lists via the customer portal.
- Ensuring that changes to emergency escalation\Maintenance contacts are communicated to Interxion Denmark ApS as soon as is practicably possible.
- Ensuring that its employees follow the "House Rules" provided in the contract and posted at CPH1+2 and CPH-RS reception.
- Ensuring that equipment is secured as necessary, including locking cages and racks. Physical security beyond the final access to the specific client rack is the sole responsibility of the client.

A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained and monitored to meet Interxion's availability commitments and requirements.

Client management is responsible for:

- Ensuring that equipment is plugged in A and B power supplies or through Static Transfer Switches (STS) equipment where applicable.

A1.1: Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet Interxion's availability commitments and requirements.

Client management is responsible for:

- Ensuring that their equipment and performance is monitored as necessary to ensure its ongoing acceptable operation.

4 Section IV: Description of Criteria, Controls, Tests and Results of Tests

4.1 Testing performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of our testing of the controls specified by Interxion, EY considered the aspects of Interxion's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

The achievement of the criteria is determined by the design, implementation and operation effectiveness of the related controls. Where deviations have been identified, we have included the extent of testing performed that led to identification of the deviation. Even after the identification of a control deviation, it is still possible to achieve the criteria.

4.2 Testing of Information Produced by the Entity

For tests of controls requiring the use of information produced by the entity (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the information produced by the entity to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the information produced by the entity, (2) inspected the query, script, or parameters used to generate the information produced by the entity, (3) tied data between the information produced by the entity and the source, and/or (4) inspected the information produced by the entity for anomalous gaps in sequence or timing to determine the data is complete and accurate. Furthermore, in addition to the above procedures, for tests of controls requiring management's use of information produced by the entity in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the source and the completeness, accuracy, and integrity of the data or reports.

4.3 Trust Services Criteria and Controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by, and are the responsibility of Interxion. The testing performed by EY and the results of tests are the responsibility of the service auditor. The following Trust Services Criteria categories are in scope of this report:

- Criteria related to Availability (applicable only to the Trust Services Criteria availability)
- Common Criteria related to Organization and Management (applicable to both the Trust Services Criteria availability and security)
- Common Criteria related to Communications (applicable to both the Trust Services Criteria availability and security)
- Common Criteria related to Risk management and design and implementation of controls (applicable to both the Trust Services Criteria availability and security)
- Common Criteria related to Monitoring of controls (applicable to both the Trust Services Criteria availability and security)
- Common Criteria related to Logical and physical access controls (applicable to both the Trust Services Criteria availability and security)
- Common Criteria related to System Operations (applicable to both the Trust Services Criteria availability and security)
- Common Criteria related to Change Management (applicable to both the Trust Services Criteria availability and security)

4.4 Criteria related to Availability

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet Interxion's availability commitments and system requirements.	**A1.1 - control A:** Operations reviews the Interxion's system capacity, availability and security performance on a monthly basis. Corrections and other necessary actions relating to identified deficiencies are taken when issues are identified.	For a sample of months, inspected the supporting documentation to determine whether the system capacity, availability and security performance were reviewed on a monthly basis and corrective actions were initiated when issues were identified by Interxion Denmark ApS Operational Management.	No deviations noted.
		A1.1 - control B: Interxion uses software to measure system utilization on systems where this is critical. Alerts are generated when specific predefined thresholds are met.	For a sample of systems, where system utilization is critical, and days, inspected the supporting documentation to determine whether each system was being monitored for service availability and capacity (system utilization) and that breaches of predefined thresholds were identified by generated alerts.	No deviations noted.
		A1.1 - control C: Capacity requirements are evaluated on signing of initial contract and on contract renewal.	Inspected power usage reports, monthly floor space reports, meeting documentation and change implementation forms to determine whether the capacity requirements on power usage and available floor space were evaluated regularly, upon signing of the initial contract and on contract renewal.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet Interxion´s availability commitments and requirements.	**A1.2 - control A**: Based on the Design Engineering Requirement and in accordance with the risk assessment, the data centre is protected against a disruption in power supply by: - Use of multiple utility power feeds - Use of Uninterruptible Power Supplies (UPS) - Generators (including fuel supply) are installed at the data centre facility, providing adequate power generation for standby continuous operation - Available data centre capacity and power load (consumption) are monitored monthly Environmental protections receive maintenance on at least an annual basis. The Design Engineering Requirement is reviewed on at least an annual basis and must be signed off by the CEO (Chief Engineering Officer) before release.	Observed the data centre and inspected supporting documentation to determine whether multiple power feeds were available and to determine whether UPS and generator systems were installed, in accordance with the Design Engineering Requirement and the risk assessment. For a sample of months, inspected the supporting documentation to determine whether the available data centre capacity and power load (consumption) were monitored on a monthly basis. For a sample of UPS and generator systems, inspected the maintenance report to determine whether maintenance has been performed on at least an annual basis. Inspected the Design Engineering Requirement document to determine whether the requirements of the data centre infrastructure were reviewed on at least an annual basis and signed off by the CEO (Chief Engineering Officer) before release.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet Interxion´s availability commitments and requirements.	**A1.2 - control B**: Based on the Design Engineering Requirement and in accordance with the risk assessment, the data centre is protected against fire by: - 24/365 monitoring of the facility on alarms by both local operations, as well as the ECSC - Smoke detection systems (including standard and VESDA) - Automatic gas-based fire suppression systems - Hand-held fire extinguishing systems - Compliance with local regulatory requirements Environmental protections receive maintenance on at least an annual basis. The Design Engineering Requirement is reviewed on at least an annual basis and must be signed off by the CEO (Chief Engineering Officer) before release.	Observed the data centre and inspected monitoring tooling and alarm documentation to determine whether smoke detection (standard and VESDA) and fire suppression (gas-based, water-based and hand-held) were installed to protect the data centre against fire, in accordance with the Design Engineering Requirement, local regulatory requirements and the risk assessment. Inquired of management, observed the data centre and inspected monitoring tooling and alarm documentation to determine whether 24/365 monitoring on fire related alarms, by local operations, was performed. Inquired of management, observed the ECSC monitoring room and inspected alarm and the ECSC monitoring shift documentation to determine whether 24/365 monitoring on fire related alarms, by the ECSC, was performed. For a sample of smoke detection (standard and VESDA) and fire suppression (gas-based, water-based and hand-held) systems, inspected the maintenance reports to determine whether maintenance has been performed on at least an annual basis. Inspected the Design Engineering Requirement document to determine whether the requirements of the data centre infrastructure were reviewed on at least an annual basis and signed off by the CEO (Chief Engineering Officer) before release.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		A1.2 - control C: Based on the Design Engineering Requirement and in accordance with the risk assessment, the data centre is protected against water leakage hazards by: - 24/365 monitoring of the facility on water detection systems by both local operations, as well as the ECSC - raised floors (if required by the risk assessment) Environmental protections receive maintenance on at least an annual basis. The Design Engineering Requirement is reviewed on at least an annual basis and must be signed off by the CEO (Chief Engineering Officer) before release.	Observed the data centre and inspected supporting documentation to determine whether floors were elevated (raised floors), if required, and water detection systems were installed to protect the data centre against water damage, in accordance with the Design Engineering Requirement and risk assessment. Inquired of management, observed the data centre, inspected monitoring tooling and alarm documentation to determine whether 24/365 monitoring on water leakage alarms, by local operations, was performed. Inquired of management and observed the ECSC monitoring room to determine whether 24/365 monitoring on water leakage alarms, by the ECSC, was performed. For a sample of water detection systems, inspected the maintenance reports to determine whether maintenance has been performed on at least an annual basis. Inspected the Design Engineering Requirement document to determine whether the requirements of the data centre infrastructure were reviewed on at least an annual basis and signed off by the CEO (Chief Engineering Officer) before release.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet Interxion´s availability commitments and requirements.	**A1.2 - control D**: Based on the Design Engineering Requirement and in accordance with the risk assessment, the entity site has a maintained and monitored climate controlled environment (which consists of CRACs, chillers etc.) by: - 24/365 monitoring of the facility for temperature by both local operations, as well as the ECSC - 24/365 monitoring of the facility for humidity by both local operations, as well as the ECSC Environmental protections receive maintenance on at least an annual basis. The Design Engineering Requirement is reviewed on at least an annual basis and must be signed off by the CEO (Chief Engineering Officer) before release.	Observed the data centre and inspected supporting documentation to determine whether climate control systems were installed to maintain and monitor the climate controlled environment, in accordance with the Design Engineering Requirement and the risk assessment. Inquired of management, observed the data centre, inspected monitoring tooling and alarm documentation to determine whether 24/365 monitoring on temperature and humidity alarms, by local operations, was performed. Inquired of management and observed the ECSC monitoring room, inspected alarm and the ECSC monitoring shift documentation to determine whether 24/365 monitoring on temperature and humidity alarms, by the ECSC, was performed. For a sample of climate control systems, inspected maintenance reports to determine whether maintenance has been performed on at least an annual basis. Inspected the Design Engineering Requirement document to determine whether the requirements of the data centre infrastructure were reviewed on at least an annual basis and signed off by the CEO (Chief Engineering Officer) before release.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		A1.2 - control E: Full and incremental back-ups are performed according to the approved back-up procedure. The back-ups are monitored on a daily basis.	Inspected the backup policy document to determine whether the requirements for the back-up process were documented and approved by the Director ICT. For a sample of in-scope systems, inspected the configuration settings of the backup schedule to determine whether the backup process was configured in line with the established backup policy. For a sample of in-scope systems and days, inspected the backup job completion report to determine whether backup completion was monitored and to determine whether any exceptions to successful backup processing were logged and followed through to resolution.	No deviations noted.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet Interxion's availability commitments and system requirements.	**A1.3 - control A**: Business Continuity procedures, including restoration of backups, are in place and are tested annually to restore the functionality in case of a disaster.	Inspected the Business Continuity procedures and inspected the annual test report of the restoration of backups to determine whether the requirements for data restoration were documented and to determine whether the restoration of back-ups was tested at least annually.	No deviations noted.
			Inspected the Business Continuity procedures to determine whether the requirements for the critical environmental protections systems in the data centre were documented. Inspected the annual Business Continuity test report, of the critical environmental protections systems in the data centre, to determine whether Interxion Denmark ApS has tested the Business Continuity procedures at least annually.	No deviations noted.
			Inspected the Business Continuity procedures to determine whether the requirements for the continuity of the customer services were documented. Inspected the annual Business Continuity test report, of the continuity of the customer services during a crisis, to determine whether Interxion has tested the Business Continuity procedures at least annually.	No deviations noted.

4.5 Common Criteria related to Organization and Management

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC1.1	Interxion has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.	**CC1.1 - control A**: Interxion has defined organizational structure, reporting lines, authorities, and responsibilities. These are revised when necessary to help meet changing commitments and requirements.	Inspected the Information Security Manual and organizational structure diagram to determine whether the organizational structure, reporting lines, authorities, and responsibilities were defined and determined that these documents were revised when necessary to meet changing commitments and requirements.	No deviations noted.
		CC1.1 - control B: Roles and responsibilities are defined in written job descriptions. The job descriptions are periodically reviewed and adjusted as needed.	Inspected the job matrix and overview of assigned job functions to determine that assigned job functions are based on job descriptions, which containing applicable roles and responsibilities, as defined in the job matrix. Inspected the job matrix and determined that job descriptions are periodically reviewed and adjusted as needed.	No deviations noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, monitoring, maintaining, and approving Interxion's system controls are assigned to individuals within Interxion with authority to ensure policies and other system requirements are effectively promulgated.	**CC1.2 - control A**: Responsibilities and accountability are defined in the security, availability and other system requirement documentation.	Inspected relevant in-scope security documentation, availability procedures and other system requirement documentation to determine whether the responsibilities and accountability were defined.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC1.3	Interxion has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability; and provides resources necessary for personnel to fulfil their responsibilities.	**CC1.3 - control A**: Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process. In order to provide that personnel responsible for the design, development, implementation, and operation of systems have the qualifications and resources to fulfil their responsibilities are in line with company guidelines and in accordance with the laws, regulations and ethics of local jurisdictions, and proportional to Interxion's business requirements and the perceived risks.	Inspected the hiring and transfer procedure to determine whether the candidates' abilities to meet the job requirements were evaluated as part of the hiring or transfer evaluation process, to ensure personnel responsible for the design, development, implementation, and operation of systems have the qualifications and resources to fulfil their responsibilities. For a sample of Interxion employees who were either hired or transferred during the audit period, inspected the job description and Recruitment Request Forms to determine whether the job requirements were documented in job descriptions. For a sample of Interxion employees who were either hired or transferred during the audit period, inspected the HR evaluation as performed on the candidates' CV and references to determine whether the candidates' abilities to meet the job requirements were evaluated as part of the hiring or transfer evaluation process.	No deviations noted.
		CC1.3 - control B: Management monitors, on a periodic basis, compliance with training requirements related to security and availability.	Inspected training compliance documentation to determine whether management monitors, on a periodic basis, compliance with training requirements related to security and availability.	Deviations noted. We determined, per inquiry with Interxion management, that the monitoring of compliancy with the training requirements is not formally documented. We cannot determine the extent of the performed management monitoring of compliance with the training requirements related to security and availability. We determined, per inspection of training session slide decks and e-mail documentation, that training sessions related to security and availability were held during the

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
				audit period and that these addressed requirements related to security and availability. No other deviations noted.
		CC1.3 - control C: Management evaluates, on a periodic basis, the need for additional resources in order to achieve business objectives.	Inspected the documented annual review by management to determine whether the available and required resources were evaluated by management to identify the need for additional resources in order to achieve the business objectives.	No deviations noted.
CC1.4	Interxion has established employee conduct standards, implemented employee candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability, where relevant.	**CC1.4 - control A**: Personnel are required to read and accept the set of rules outlining the responsibilities and ethics and the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them periodically thereafter.	For a sample of Interxion employees, inspected the Acceptable Use Policy registration documentation to determine whether personnel has read and accepted the set of rules outlining the responsibilities, ethics, confidentiality and privacy practices to determine whether these were reaffirmed and monitoring by management was performed.	No deviations noted.
		CC1.4 - control B: Hiring procedures include background checks or reference validation.	Inspected the hiring procedure to determine whether the requirement for background checks or reference validation. For a sample of Interxion employees who were either hired or transferred during the audit period, inspected supporting documentation to determine whether a background check or reference validation was performed to enable Interxion to meet the security and availability commitments and requirements.	No deviations noted.

4.6 Common Criteria related to Communications

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	**CC2.1 - control A**: A formally documented system description is made available to authorized external users via the welcome pack and made available to internal users on the intranet.	Inspected the welcome pack to determine whether the relevant procedures regarding the design and operation of the system (formal system description) were available to the authorized external users. Inspected the intranet website to determine whether the relevant procedures regarding the design and operation of the system (formal system description) was available to the authorized internal users.	No deviations noted.
CC2.2	Interxion's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities	**CC2.2 – control A**: Employees of Interxion state their responsibility for information security and receive appropriate awareness training and regular updates in organizational policies and procedures that are relevant for their job function.	Inspected the Acceptable Use Policy to determine whether security commitments were included. For a sample of Interxion employees who were either hired or transferred during the audit period, inspected the Acceptable Use Policy registration documentation to determine whether confirmation of their responsibility for information security was available. For a sample of Interxion employees, inspected the Acceptable Use Policy registration documentation to determine whether reaffirmation of their responsibility for information security was available.	No deviations noted.
			Inquired of management to determine whether training on security awareness and organizational policies and procedures was provided to Interxion employees. Inspected the attendance lists and training documentation to determine whether Interxion employees have attended the training on security awareness and organizational policies and procedures.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		CC2.2 – control B: Customers / clients receive a standard introductory welcome pack containing key information around the data centre facility responsibilities. The Service Level Agreement, which includes Interxion's responsibilities, is communicated to customers upon signing the initial contract.	Inspected the introductory welcome pack and Service Level Agreement to determine whether the documents contain key information around the data centre facility responsibilities and contain Interxion's responsibilities to enable customers to carry out their responsibilities. For a sample of new Interxion customers, inspected the communication of the introductory welcome pack to determine whether the welcome pack was communicated to the customer. For a sample of new Interxion customers, inspected the communication of the Service Level Agreement (SLA) to determine whether the SLA was communicated to customers upon signing the initial contract.	No deviations noted.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	**CC2.3 – control A**: Interxion has clearly defined security and availability responsibilities which are published to the internal users.	Inspected the relevant security and availability policies and procedures to determine whether responsibilities of internal users were defined. Inspected the intranet website to determine whether the relevant security and availability policies and procedures were published and accessible to the internal users.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		CC2.3 - Control B: Customers / clients receive a standard introductory welcome pack containing key information around the data centre facility responsibilities. The Service Level Agreement, which includes Interxion's responsibilities, is communicated to customers upon signing the initial contract.	Inspected the introductory welcome pack and the Service Level Agreement (SLA) to determine whether the documents contain key information around the data centre facility responsibilities and contain Interxion's responsibilities to enable customers to carry out their responsibilities. For a sample of new Interxion customers, inspected the communication of the introductory welcome pack to determine whether the welcome pack was communicated to the customer. For a sample of new Interxion customers, inspected the communication of the Service Level Agreement (SLA) to determine whether the SLA was communicated to customers upon signing the initial contract.	No deviations noted.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.	**CC2.4 - control A**: Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are published and available on the intranet.	Inspected the relevant security and availability policies and procedures to determine whether responsibilities of internal users were defined. Inspected the intranet website to determine whether the relevant security and availability policies and procedures were published and accessible to the internal users.	No deviations noted.
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	**CC2.5 - control A**: Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are published and available on the intranet.	Inspected the relevant security and availability policies and procedures to determine whether the responsibilities for reporting operational failures, incidents, system problems, concerns, and user complaints were defined. Inspected the intranet website and document sharing tool to determine whether the relevant security and availability policies and procedures were published and accessible.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		CC2.5 - control B: Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described in the welcome pack.	Inspected the most recent version of the welcome pack to determine whether the responsibilities for reporting operational failures, incidents, system problems, concerns, and user complaints were defined.	No deviations noted.
CC2.6	System changes that affect internal and external users' responsibilities or Interxion's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	**CC2.6 - control A**: Changes that may impact system availability and related system security are communicated to affected customers and internal users before implementation of the proposed change.	For a sample of changes inspected the related Customer Communication notifications to the affected customers and internal users, to determine whether the change was communicated before implementation.	No deviations noted.

4.7 Common Criteria related to Risk management and design and implementation of controls

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC3.1	Interxion (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyses the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and	**CC3.1 – control A**: Interxion has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Procedures are in place that sets out the measures taken to address the associated risks.	Inquired of management to determine whether the risk management process specified (standard) risk tolerances and was based on identified risks. Inspected the risk management procedures to determine whether risk tolerances, the process for evaluating risks taken to address the associated risks were specified. Inspected the annual risk assessments, based on the risk management template, to determine whether risks were evaluated based on identified threats and risk tolerances and to determine whether measures were specified to address the identified risks.	No deviations noted.
		CC3.1 – control B: A business recovery plan is in place for each data centre and is reviewed annually by local management.	Inspected the business recovery plans for the data centres in scope to determine whether the procedure was in place and annually reviewed by Interxion Denmark ApS management.	No deviations noted.
		CC3.1 - control C: During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the risk management procedures and the annual risk assessments to determine whether changes in business objectives, commitments and requirements, internal operations and external factors were identified and included as potential threats to the system objectives.	No deviations noted.
		CC3.1 - control D: On a periodic basis meetings are held to discuss security and availability concerns and trends related to data centre facilities, as well as upcoming business or new technologies that may impact the data centre security and availability.	Inquired of management to determine whether periodic meetings were held to discuss security and availability concerns and trends. For a sample of weeks, inspected the meeting documentation of the Operational Management meetings to determine whether the security and availability concerns, trends, technologies and upcoming business relevant to the data centre security and availability were discussed.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
	revises, as necessary, risk assessments and mitigation strategies based on the identified changes.			
CC3.2	Interxion designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	**CC3.2 – control A**: Interxion's Senior Management Team annually reviews and approves the Interxion Security and Availability policies and procedures. Interxion has published it to employees and shall do so to relevant external parties on request. Local consultation is carried out within Interxion by the Information Security Committee (INFOSEC). Updates to security and availability policies and procedures were initiated by management when required.	Inquired of management to determine whether the security and availability policies and procedures were reviewed annually and after changes that could impact stakeholders. Inspected the security and availability policies and procedures and inspected the SharePoint environment to determine whether these policies and procedures were annually reviewed and approved by Interxion's Senior Management team to ensure policies and procedures were up-to-date. Inquired of management and inspected the SharePoint environment to determine whether Interxion Security and Availability policies and procedures were published to relevant external parties on request. Inspected meeting documentation to determine whether local consultations were carried out within Interxion by the Information Security Committee (INFOSEC) on a quarterly basis.	No deviations noted.
		CC3.2 - control B: Vulnerability scans on physical (annual audits are performed on physical security at data centres) and logical (penetration tests) access level are performed on an annual basis.	Inspected the relevant physical access policies and procedures to determine whether the requirement, to perform an annual vulnerability scan on physical access level (physical security audit), was included. Inspected the annual physical security audit report for the data centres in scope to determine whether a vulnerability scan on physical access level (physical security audit) has been performed.	No deviations noted.
			Inspected the relevant logical access policies and procedures to determine whether the requirement, to perform an annual vulnerability scan on logical access level (penetration tests), was included.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
			Inspected the annual penetration test and the annual performed security review to determine whether vulnerability scans on logical access level have been performed.	
		CC3.2 - control C: Interxion has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Procedures are in place that sets out the measures taken to address the associated risks.	Inquired of management to determine whether the risk management process specified (standard) risk tolerances and was based on identified risks. Inspected the risk management procedures to determine whether risk tolerances, the process for evaluating risks taken to address the associated risks were specified. Inspected the annual risk assessments, based on the risk management template, to determine whether risks were evaluated based on identified threats and risk tolerances and to determine whether measures were specified to address the identified risks.	No deviations noted.
		CC3.2 – control D: During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the risk management procedures and the annual risk assessments to determine whether changes in business objectives, commitments and requirements, internal operations and external factors were identified and included as potential threats to the system objectives.	No deviations noted.

4.8 Common Criteria related to Monitoring of controls

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC4.1	The design and operating effectiveness of controls are periodically evaluated against Interxion's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	**CC4.1 - control A**: Operations reviews the Interxion's system capacity, availability and security performance on a monthly basis. Corrections and other necessary actions relating to identified deficiencies are taken when issues are identified.	For a sample of months, inspected the supporting documentation to determine whether the system capacity, availability and security performance were reviewed and corrective actions were initiated when issues were identified by Interxion Denmark ApS Operational Management.	No deviations noted.
		CC4.1 - control B: Logging and monitoring software is used to collect data of security and availability breaches and incidents due to malicious acts, natural disasters, or errors. In case of breaches and incidents appropriate follow-up is performed.	Inspected monitoring software tools to determine whether data was logged on security and availability breaches and incidents due to malicious acts, natural disasters, or errors on systems. For a sample of in-scope systems and days, inspected the supporting documentation to determine whether each system was being monitored on capacity and availability issues appropriate follow-up actions were taken. For a sample of days, inspected the daily Intrusion Prevention System (IPS) monitoring report to determine whether security breaches were identified and appropriate follow-up actions were taken.	No deviations noted.
			Observed the date centre and inspected supporting documentation to determine whether environmental protection systems were installed to monitor or detect temperature, humidity, water leakage, power load, physical security and fire. For a sample of security and availability alarms of the environmental protection systems in the data centre, inspected the incident ticket and e-mail communication, to determine whether the appropriate follow-up has been taken, including customer communication notification (if appropriate).	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		CC4.1 - control C: There is a periodic meeting with the data centre operation managers and the VP operations support to identify and address potential impairments to the entity's ongoing ability to achieve its objectives. If impairments are identified specific projects are set up to resolve those.	Inquired of management to determine whether periodic meetings were held between the operation managers and the VP Operations Support to identify and address potential impairments to the entity's ongoing ability to achieve its objectives and if impairments were identified specific projects were set up to resolve those For a sample of months, inspected the meeting documentation of the Operational Management meetings to determine whether potential impairments to Interxion's ongoing ability to achieve its objectives were identified and addressed.	No deviations noted.
		CC4.1 – control D: On an annual basis a penetration test is performed. Any issues identified are evaluated and follow-up actions are documented.	Inspected the relevant logical access policies and procedures to determine whether the requirement, to perform an annual penetration test, was included. Inspected the annual performed security review to determine whether an annual penetration test has been performed, issues were identified and follow-up actions were documented.	No deviations noted.

4.9 Common Criteria related to Logical and physical access controls

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet Interxion's commitments and system requirements as they relate to security and availability.	**CC5.1 - control A**: Infrastructure components and software are required to be implemented with password submission and separate user ID (where possible).	Inspected the relevant logical access policies and procedures to determine whether a process, for password submission and usage of separate user ID's, is formalized. For a sample of in-scope systems, inspected Active Directory Single Sign-On (SSO) documentation to determine whether the submission of a password and separate user ID was required to access these systems. For applications inspected user account listings, authorization matrices and supporting documentation to determine whether the submission of a password and separate user ID was required to access these applications. In case generic application accounts were required, inspected supporting documentation to determine whether the use of generic accounts was limited to authorized personnel.	No deviations noted.
		CC5.1 – control B: When possible, formal role-based access controls limit access to system and infrastructure components are created and these are enforced by the access control system.	Inspected authorization listings and authorization matrices to determine whether authorizations were assigned and enforced by the access control system.	No deviations noted.
		CC5.1 - control C: External points of connectivity are protected by a firewall complex and an Intrusion Prevention System.	Inspected the monitoring documentation of the firewall and Intrusion Prevention System (IPS) to determine whether the external points of connectivity were protected and monitored to protect the Interxion environment against security and availability threats.	No deviations noted.
CC5.2	New internal and external users, whose access is administered by Interxion, are registered and authorized prior to being issued system credentials and granted the ability to	**CC5.2 – control A**: There is a formal user registration and de-registration procedure, for those whose access is administered by the entity for granting and revoking access to all information systems and services.	Inspected the relevant logical access policies and procedures to determine whether the user registration and de-registration procedure was formalized. For a sample of granted access for internal and external users as created during the audit period, inspected the supporting documentation to determine whether the request	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
	access the system to meet Interxion's commitments and system requirements as they relate to security and availability. For those users whose access is administered by Interxion, user system credentials are removed when user access is no longer authorized.		was recorded and approval by appropriate management, for the assigned access and authorizations, was available for all in scope systems. For a sample of internal and external users who left the Interxion organization during the audit period, inspected the supporting documentation to determine whether the request was recorded and access was revoked for in scope systems.	
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet Interxion's commitments and system requirements as they relate to security and availability.	**CC5.3 – control A**: All users have a unique identifier (user ID) for their personal and sole use and a password authentication technique has been chosen to substantiate the claimed identity of a user. On network level all accounts are uniquely identifiable, while on application generic accounts are in place if required. Two factor authentication is used for external access to the Interxion network.	Inspected the relevant logical access policies and procedures to determine whether a process, on identifying and authenticating users, is formalized. Inspected user account listings, authorization matrices and supporting documentation to determine whether user accounts of the in scope systems had unique identifiers assigned and password authentication techniques were used to substantiate the claimed identity of a user. In case generic application accounts were required, inspected supporting documentation to determine whether the use of generic accounts was limited to authorized personnel. Inspected authentication tools and observed the use of two factor authentication to determine whether two-factor authentication is used for external access to the Interxion network.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet Interxion's commitments and system requirements as they relate to security and availability	**CC5.4 – control A**: Management reviews users' access rights, of which privileged access, at regular intervals using the formal process. Access change requests resulting from the review are submitted to the responsible security group via a change request record.	Inspected the relevant logical access policies and procedures to determine whether a management review process, on users' access rights and privileged access, was formalized. Inspected the management review documentation to determine whether the management review, on users' access rights and privileged access, was performed at regulated intervals on in scope systems. Inspected the management review documentation to determine that change requests, resulting from the review on user's access rights and privileged access for in scope systems, were documented and were submitted to the responsible security group by means of a change request.	No deviations noted.
		CC5.4 – control B: When possible, formal role-based access controls limit access to system and infrastructure components and these are enforced by the access control system.	Inspected authorization listings and authorization matrices to determine whether authorizations were assigned to specific roles for in scope systems.	No deviations noted.
		CC5.4 – control C: There is a formal user registration and de-registration procedure, for those whose access is administered by the entity for granting and revoking access to all information systems and services.	Inspected the relevant logical access policies and procedures to determine whether the user registration and de-registration procedure was formalized. For a sample of granted access for internal and external users during the audit period, inspected the supporting documentation to determine whether the request was recorded and approval by appropriate management, for the assigned access and authorizations, was available for all in scope systems. For a sample of internal and external users who left the Interxion organization, inspected the supporting documentation to determine whether the request was recorded and access was revoked for in scope systems.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC5.5	Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet Interxion's commitments and system requirements as they relate to security and availability.	**CC5.5 – control A**: Formal procedures are in place for granting access to the data centre for temporary contractors and visiting customers. These procedures include, but are not limited to, the following: - process of requesting access to the data centre - identification on site of contractor against registered ID - authorization matrix showing all restricted areas - house rules that have to be read before entering site	Inspected the relevant physical security policies and procedures to determine whether formal procedures were in place for granting access to the data centre for temporary contractors and visiting customers. Inspected the relevant physical security policies and procedures to determine whether the following sections were available: process description of requesting access, ID identification requirement, authorization matrix with restricted areas and the house rules. For a sample of access requests, for visiting customers, inspected the Sage CRM request ticket, visitor log and badge access log to determine whether the request was recorded and approval by the ECSC, for the granted access, was available and in accordance with the formal procedures. For a sample of access requests, for temporary contractors, inspected the Ultimo Work order, visitor log and badge access log to determine whether the request was recorded and approval by local management, for the granted access, was available and in accordance with the formal procedures.	No deviations noted.
		CC5.5 – control B: The physical security of the data centre includes, but are not limited to, the following: - Secured rooms, cages and cabinets with keys or access badges - Surveillance cameras covering the whole perimeter (in and around building) - Alarm system (sound and visual) - Infrared sensors - Security staff on site 24/7 - Redundant outside telephone lines Annual audits are performed on physical security of the data centre.	Inquired of management, inspected supporting documentation and observed the data centres in scope to determine whether the required security measures were present. Inspected the relevant physical access policies and procedures to determine whether the requirement, to perform an annual vulnerability scan on physical access level (physical security audit), was included. Inspected the annual physical security audit report for the data centres in scope to determine whether a vulnerability scan on physical access level (physical security audit) has been performed.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
		CC5.5 – control C: All new, changed or revoked permanent physical access rights are requested using a central process managed by Interxion's European Customer Service Centre (ECSC). Access is validated by an ECSC agent before access is granted.	Inspected the relevant physical security policies and procedures to determine whether formal procedures were in place for granting, updating and revoking permanent access to the data centre for employees and customers. For a sample of granted and changed permanent physical access rights, inspected the request ticket, approval of the ECSC and badge access logs to determine whether the request was recorded and approval by the ECSC, for the granted permanent access, was available and in accordance with the formal procedures. For a sample of requests to revoke permanent physical access, inspected the request ticket, notification to the security guards and badge access logs to determine whether the permanent access to the data centre was timely revoked.	No deviations noted.
		CC5.5 – control D: Physical access rights for all Interxion staff and third parties are reviewed annually to ensure that access rights are accurate, valid and assigned restrictively (least privilege principle).	Inspected the relevant physical security policies and procedures to determine whether formal procedures were in place for reviewing physical access rights. Inspected the annual physical access rights management review to determine whether the granted physical access of Interxion staff and third parties were accurate, valid and assigned restrictively.	No deviations noted.
		CC5.5 – control E: The sharing of access badges and tailgating are prohibited by policy.	Inspected the relevant physical security policies and procedures to determine whether formal procedures were in place which prohibit sharing of access badges and tailgating.	No deviations noted.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet Interxion's commitments and system requirements	**CC5.6 - control A**: External points of connectivity are protected by a firewall complex and an Intrusion Prevention System.	Inspected the monitoring documentation of the firewall and Intrusion Prevention System (IPS) to determine whether the external points of connectivity were protected and monitored to protect the Interxion environment against security and availability threats.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling Interxion to meet its commitments and system requirements as they relate to security and availability.	**CC5.7 - control A**: Interxion security policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted and prohibits storing data on removable media to internal and external users.	Inspected the relevant security policies and procedures to determine whether the process was formalized to prohibit the transmission of sensitive information over public communications paths, unless the information is encrypted, and to prohibit storing data on removable media to internal and external users.	No deviations noted.
		CC5.7 - control B: Two factor authentication is used for external access.	Inspected authentication tools and observed the use of two factor authentication for external access to the Interxion network.	No deviations noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet Interxion's commitments and system requirements as they relate to security and availability	**CC5.8 - control A**: Anti-virus software is installed on workstations, laptops, and systems supporting such software. The software is updated on a periodic basis. A report of devices that have not been updated for a certain amount of days is reviewed on a periodic basis and follow up actions are taken.	Inspected the OfficeScan monitoring tool and compliancy reports to determine whether workstations, laptops, and systems were monitored to ensure anti-virus definitions were installed and regularly updated. For a sample of months inspected service request ticket documentation and compliancy reports to determine whether a periodic review was performed by an ICT employee to identify workstations, laptops, and systems containing either outdated anti-virus definitions or on which the anti-virus scan did not ran for several months. For these exceptions we determined per inspection of OfficeScan information, as stored in a data warehouse, that appropriate follow-up actions were taken.	No deviations noted.

4.10 Common Criteria related to System Operations

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet Interxion's commitments and system requirements as they relate to security and availability.	**CC6.1 - control A**: Logging and monitoring software is used to collect data of security and availability breaches and incidents due to malicious acts, natural disasters, or errors. In case of breaches and incidents appropriate follow-up is performed.	Inspected monitoring software tools to determine whether data was logged on security and availability breaches and incidents due to malicious acts, natural disasters, or errors on systems. For a sample of in-scope systems and days, inspected the supporting documentation to determine whether each system was being monitored on capacity and availability issues appropriate follow-up actions were taken. For a sample of days, inspected the daily Intrusion Prevention System (IPS) monitoring report to determine whether security breaches were identified and appropriate follow-up actions were taken.	No deviations noted.
			Observed the date centre and inspected supporting documentation to determine whether environmental protection systems were installed to monitor or detect temperature, humidity, water leakage, power load, physical security and fire. For a sample of security and availability alarms of the environmental protection systems in the data centre, inspected the incident ticket and e-mail communication, to determine whether the appropriate follow-up has been taken, including customer communication notification (if appropriate).	No deviations noted.
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with	**CC6.2 - control A**: Personnel follow defined protocols for evaluating reported security and availability breaches and incidents. Security related breaches and incidents are assigned to the security / operations group for impact evaluation. Operations and security personnel follow defined protocols for resolving and	Inspected the relevant incident management policies and procedures to determine whether formal procedures were in place for evaluating reported logical security and availability breaches and incidents. Inspected the relevant incident management policies and procedures to determine whether roles and responsibilities were defined and specify which security / operations groups	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
	established incident response procedures to meet Interxion's commitments and system requirements.	escalating security and availability breaches and incidents.	were responsible for evaluating the impact of logical security and availability breaches and incidents. For a sample of logical security and availability alarms of the in scope IT systems, inspected the TOPdesk incident ticket and e-mail communication to determine whether the defined protocol has been followed for logical security and availability breaches and incidents. For a sample of logical security and availability alarms of the environmental protection systems in the data centre, escalated to the ECSC, inspected the CRM incident ticket and e-mail communication to determine whether the defined protocol has been followed for physical security and availability breaches and incidents.	
			Inspected the relevant incident management policies and procedures to determine whether formal procedures were in place for evaluating reported physical security and availability breaches and incidents. Inspected the relevant incident management policies and procedures to determine whether roles and responsibilities were defined and specify which security / operations groups were responsible for evaluating the impact of physical security and availability breaches and incidents. For a sample of daily guard reports, containing logging on physical security and availability alarms of the environmental protection systems in the data centre, escalated to the ECSC, inspected the type of incident and follow-up actions to determine whether the defined protocol has been followed for physical security and availability breaches and incidents.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet Interxion's commitments and system requirements.	**CC6.2 - control B**: The resolution of security and availability breaches and incidents is reviewed at regular operations and security group meetings. Relevant security and availability breaches and incidents, with user or customer impact, are referred to user and customer care management to be addressed.	For a sample of quarters, inspected the quarterly report and Operations (OPS) meeting documentation to determine whether resolution of relevant security and availability breaches and incidents, with customer impact, were reviewed regularly by HQ level (operations and security) group meetings attended by customer care management, VP Operations Support and local operational managers.	No deviations noted.
			For a sample of months, inspected the meeting documentation of the monthly Interxion Denmark ApS operations and security group meetings to determine whether the resolution of security and availability breaches and incidents were reviewed and discussed.	No deviations noted.

4.11 Common Criteria related to Change Management

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC7.1	Interxion commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	**CC7.1 - control A**: The implementation of changes to data centre infrastructure or monitoring systems are evaluated to determine the potential impact of the change on security and availability commitments and requirements. Changes are appropriately authorized and approved.	Inspected the relevant change management procedure to determine whether formal procedures were in place for implementing changes to data centre infrastructure or monitoring systems and roles and responsibilities were defined. For a sample of changes to data centre infrastructure or monitoring systems, inspected the Request for Change (RfC) form and e-mail communication to determine whether changes were appropriately authorized, approved and evaluated to determine the potential impact on security and availability commitments and requirements.	No deviations noted.
CC7.2	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet Interxion's commitments and system requirements as they relate to security and availability.	**CC7.2 - control A**: During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests and / or business cases are created based on the identified needs.	Inspected the HQ ICT risk assessment and the HQ ICT planning and budgeting process documentation to determine whether IT infrastructure, data, software and procedures were evaluated to identify required changes to remain consistent with security and availability commitments and requirements.	No deviations noted.
			Inspected the Interxion Denmark ApS risk assessment, project tracking and local periodic planning and budgeting process documentation to determine whether physical infrastructure and procedures were evaluated to identify required changes to remain consistent with security and availability commitments and requirements. Inspected an Interxion Denmark ApS project to determine whether change requests and / or business cases were created for the identified and required changes.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Test of Controls performed by EY	Results of Tests
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	**CC7.3 - control A**: For incidents which are classified as 'high severity incidents' by Interxion change tickets are created and the change management process is initiated.	For a sample of high severity incidents, inspected the CRM incident ticket, e-mail communication and change management ticket to determine whether an emergency change ticket was created and appropriately documented.	No deviations noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet Interxion's security and availability commitments and system requirements.	**CC7.4 - control A**: Changes to the data centre that impact the customer, infrastructure or monitoring systems are tested and approved by senior management prior to installation in accordance with Interxion change management procedures.	For a sample of changes to data centre infrastructure or monitoring systems that potentially impact the customer, inspected the Request for Change (RfC) form and e-mail communication containing approvals to determine whether the change was approved by senior management (the Change Approval Board (CAB) and the change administrator) and a DT&EG approved test plan was available before implementation.	No deviations noted.
			For a sample of changes to data centre infrastructure or monitoring systems that potentially impact the customer, inspected the signed-off test plan by the Interxion Denmark ApS engineer to determine whether the change was tested before implementation in accordance with Interxion change management procedures.	No deviations noted.

5 Section V: Other Information Provided by Interxion Denmark ApS

5.1 Interxion Denmark ApS Operational Excellence

Interxion Denmark ApS are certified for the ISO 27001 standard for Information Security Management System and for the ISO 22301 standard for Business Continuity Management. In addition to these certifications, Interxion Denmark ApS is involved in multiple programs and initiatives with a focus on energy efficiency and green IT.

5.2 Energy Efficiency

Interxion is committed to work with energy efficiency measures in a controlled and documented structure. Interxion align our services to follow the guidelines from ASHRAE for server inlet temperature and humidity. Energy measures i.e. for PUE are defined, implemented, measured, and reported monthly to Interxion HQ. In 2015 Interxion Denmark ApS commissioned groundwater cooling as a supplement to existing cooling installation. In addition, Interxion Denmark ApS purchases 100% green energy for its data centres.

5.3 CPH2: new build, same standards

During the reporting period of this SOC2 report, Interxion continued the build for a new data centre named CPH2.2. CPH2.1 (first phase of the data centre was operational in Q2 2016) and CPH2.2 will become operational in Q1 2017.

5.4 Waste Management & Environmental Care

Interxion takes responsibility in managing waste from our customers. Interxion has prepared specific waste management procedures and dedicated waste stations on all data centres to facilitate separated and secure waste collection.

5.5 Maintenance Management

Maintenance of data centre equipment can make the difference in achieving uptime for customers. Interxion maintains an extensive preventive maintenance program, managed and supervised by Interxion, following manufacturer guidelines and specifications. Maintenance work follows strict procedures is subject to the change management process. The Interxion Denmark ApS Operations team includes a specific Facility team, led by a dedicated Facility Manager. Interxion Denmark ApS implemented an advanced Maintenance Management System to manage, plan and document all maintenance activities, including an extensive asset database.