Interxion

Interxion Deutschland GmbH

Service Organisation Controls (SOC) 2 Report

Report on Interxion Deutschland GmbH 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
July 1, 2019 to December 31, 2019

interxion™

interxion™

Contents

1 Section I: Interxion Deutschland GmbH's Management Statement

We have prepared the accompanying "Interxion's cloud and carrier colocation data centre services system operated in Germany for the period July 1, 2019 to December 31, 2019" (Description) of Interxion Deutschland GmbH (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the cloud and carrier colocation data centre services system (System) that may be useful when assessing the risks arising from interactions with the System throughout the period July 1, 2019 to December 31, 2019, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security and availability set forth in TSP section 100, *2017 Trust Services 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 presents the System that was designed and implemented throughout the period July 1, 2019 to December 31, 2019 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described throughout the period July 1, 2019 to December 31, 2019.

c. The Service Organization's controls stated in the Description operated effectively throughout the period July 1, 2019 to December 31, 2019 to achieve the service commitments and system requirements based on the applicable trust services criteria.

Qualification

As noted in Section IV of this report, controls related to the following Trust Services Criteria category: Common Criteria related to Logical and Physical access were not operating effectively during the period July 1, 2019 to December 31, 2019 to achieve the following Trust Services Criteria:

- CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
- CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Frankfurt, Germany, February 7, 2020

Interxion Deutschland GmbH

Jens Prautzsch

Managing Director /
Director Operations

Building a better working world

2 Section II: Assurance Report of the independent Service Auditor

To: management of Interxion Deutschland GmbH

Our qualified opinion

We have examined Interxion Deutschland GmbH's accompanying "Interxion's cloud and carrier colocation data centre services system operated in Germany for the period July 1, 2019 to December 31, 2019" of its the cloud and carrier colocation data centre services system for providing colocation data centre services throughout the period July 1, 2019 to December 31, 2019 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period July 1, 2019 to December 31, 2019 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security and availability, set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

In our opinion, except for the matter described in the 'Basis for our Qualified Opinion' section, in all material respects:

a. the Description presents the System that was designed and implemented throughout the period July 1, 2019 to December 31, 2019 in accordance with the Description Criteria.
b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively throughout the period July 1, 2019 to December 31, 2019.
c. the controls operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust service criteria throughout the period July 1, 2019 to December 31, 2019.

The criteria applied in forming our opinion are the criteria described in "Interxion Deutschland GmbH's Management Statement" (Management Statement).

Our opinion has been formed on the basis of the matters outlined in this assurance report. 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).

Basis for our qualified opinion

Interxion Deutschland GmbH states in its Description that it has controls in place to provide reasonable assurance that the applicable trust services criteria category for Logical and Physical Access would be met if the controls operated effectively. However, controls CC6.4 – control A/CC6.5 – control A and CC6.4 – control C/CC6.5 – control C were not operating effectively throughout the period from July 1, 2019 to December 31, 2019. This resulted in the non-achievement of the following Trust Service Criteria:

- CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

- CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

We performed our examination in accordance with Dutch law and Dutch Guideline 3000A 'Assurance-opdrachten door IT Auditors (attest-opdrachten)' (Assurance engagements performed by IT Auditors (attestation engagements) as issued by the professional association for IT-auditors in the Netherlands (NOREA) and in accordance with International Standard on Assurance Engagements 3000, 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information'. This engagement is aimed to obtain reasonable assurance. Our responsibilities in this regard are further described in the 'Service auditor's responsibilities' section of our assurance report.

We have complied with the NOREA 'Reglement Gedragscode' (Code of Ethics for IT-Auditors, a regulation with respect to integrity, objectivity, professional competence and due care, confidentiality and professional behavior) and with the 'Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten' (ViO, Code of Ethics for Professional Accountants, a regulation with respect to independence). The Code of Ethics for IT-Auditors and the NOREA Guidelines related to assurance engagements are at least as demanding as the International Code of Ethics for Professional Accountants (including International Independence Standards) of the International Ethics Standards Board for Accountants (the IESBA Code).

We believe that the assurance evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Matters related to the scope of our examination

Other information provided by Interxion Deutschland GmbH Management:

The information in the accompanying "Other information provided by Interxion Deutschland GmbH Management" is presented by management of Interxion Deutschland GmbH to provide additional information and is not a part of Interxion Deutschland GmbH's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Our opinion is not modified in respect of these matters.

Limitations of the Description and to controls at a service organization

The Description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not 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.

Restrictions on use and distribution

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 Deutschland GmbH, user entities of Interxion Deutschland GmbH's cloud and carrier colocation data centre services system during some

or all of the period July 1, 2019 to December 31, 2019 and prospective user entities, independent auditors and practitioners providing services to such user entities 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
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Our assurance report, including the Description of Tests and Results, should only be used for the intended purpose by the intended users. Without our prior written consent, it is not allowed to publish or distribute this document to others, in whole or in part, or to quote from or refer to our assurance-report or the Description of Tests and Results, whether or not with acknowledgement.

Responsibilities of management of service organization

Interxion Deutschland GmbH is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. Interxion Deutschland GmbH has provided the accompanying statement titled, "Interxion Deutschland GmbH's Management Statement" (Management Statement) 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 provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Interxion Deutschland GmbH 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) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

Service auditor's responsibilities

Our responsibility is to plan and perform our examination in a manner that allows us to obtain sufficient and appropriate assurance evidence of our opinion on the presentation of the Description 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.

Our examination has been performed with a high, but not absolute, level of assurance, which means we may not detect all material errors and fraud during our examination.

We apply the Reglement Kwaliteitsbeheersing NOREA (RKBN, a standard on quality control) that is at least as demanding as the International Standard on Quality Control 1 (ISQC 1), 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.

We planned and performed our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Amsterdam, February 7, 2020
Ernst & Young Accountants LLP

Dennis Houtekamer

Digitaal ondertekend door Dennis Houtekamer
DN: cn=Dennis Houtekamer, c=NL, o=Ernst & Young Accountants LLP, email=dennis.houtekamer@nl.ey.com
Datum: 2020.02.07 14:03:51 +01'00'

drs. D. Houtekamer RE
Associate Partner

Document reference: RITM3579735

3 Section III: Interxion's cloud and carrier colocation data centre services system operated in Germany for the period July 1, 2019 to December 31, 2019

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 Deutschland GmbH 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 over 50 data centres across 13 cities in 11 countries (Amsterdam, London, Copenhagen, Stockholm, Frankfurt, Düsseldorf, Vienna, Paris, Marseille, Dublin, Brussels, Madrid and Zurich). The head office is located in Hoofddorp, the Netherlands.

The Data centres are strategically located to ensure they have excellent power availability and connectivity. Interxion houses more than 650 carriers and Internet service providers and more than 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 Deutschland GmbH was founded in 1999 and its cloud and carrier neutral colocation data centre services are provided in their data centres. Interxion Deutschland GmbH geographic accessibility allows comprehensive cable infrastructure access to worldwide telecommunications networks.

3.1.3 Service commitments

Interxion provides an industry-leading level of service excellence by understanding its customers' requirements, efficiently and effectively dealing with those requirements, building their trust through open and proactive communication, and delivering a consistent, friction-free experience.

Interxion has defined the following principle service commitments:

- Interxion is committed to maintain 99,999% uptime.
- Interxion is committed to provide a vulnerability-controlled ICT system within logical and physically controlled environments
- Interxion is committed to meet agreed Service Organization SLA's.
    - **Service Level Power: Advanced Power / Standard Power:** Two socket outlets per cabinet. AC single phase and AC three phases: One socket is supplied by an uninterrupted power supply (UPS) system. The other socket, serving as back-up, is supplied by a sperate but identical UPS system. Input power for the two UPS systems is provided by the commercial power supply system, which is backed-up by stand-by generators.
    - **Service Level climate control:** Climate control maintains the temperature and humidity in the Customer space.
    - **Service Level Hands & Eyes Services:** An engineer will be available to respond to Customer requests for assistance within the agreed response time.
    - **Service Level Cross Connect Services:** Time to Repair (TtR, or the time between a service outage reported by the Customer by notice to the ECSC and the time of a Service restoration by Interxion.
    - **Service Level Cloud Connect Services:** Cloud Service available and passing traffic from at least one Cloud Access at any given time as determined from the Customer's Cloud Access port on the Cloud Connect Platform to the CSP Interface on the Cloud Connect Platform.
    - **Cloud Service Availability:** Cloud Service available and passing traffic from at least one Cloud Access in a configuration of two Cloud Access (redundant setting) at any given time as determined from the Customer's Cloud Access port on the Cloud Connect Platform to the CSP Interface on the Cloud Connect Platform.
- Interxion is committed to maintain industry standard certifications and compliance programs in relevant entities, including ISO27001, ISO22301, SOC2 Type II, PCI-DSS (refer to 3.3.4 – page 26).

3.1.4 System requirements

The system requirements, for achieving the Service Commitments, commitments to vendors and business partners, compliance with relevant laws and regulations and industry standard certifications and compliance programs, are documented within Interxion documented system policies and procedures, system design documentation and contracts with customers.

In order to maintain system specification effectiveness, risk based recurring testing is performed to ensure continual improvement. The key system requirements that are applicable for the Interxion's services in scope are described in the following table and include references to the sections containing the system requirements:

Key service commitments	Relevant section(s)
Interxion is committed to maintain 99,999% uptime	3.3.1 Control environment 3.3.3 Risk Assessment 3.3.4 Monitoring Activities 3.3.7 System Operations 3.3.8 Change Management 3.3.9 Risk Mitigation

Key service commitments	Relevant section(s)
	3.3.10 Availability – Additional Criteria
Interxion is committed to provide a vulnerability-controlled ICT system within logical and physically controlled environments	3.3.1 Control environment 3.3.3 Risk Assessment 3.3.4 Monitoring Activities 3.3.5 Control Activities 3.3.6 Logical & Physical Access Control 3.3.7 System Operations 3.3.8 Change Management 3.3.9 Risk Mitigation 3.3.10 Availability
Interxion is committed to meet agreed Service Organization SLA's.	3.3.1 Control environment 3.3.2 Communication and Information 3.3.3 Risk Assessment 3.3.4 Monitoring Activities 3.3.5 Control Activities 3.3.6 Logical & Physical Access Control 3.3.7 System Operations 3.3.8 Change Management 3.3.9 Risk Mitigation 3.3.10 Availability
Service Level Power: Advanced Power / Standard Power	3.3.5 Control Activities
Service Level climate control	3.3.5 Control Activities
Service Level Hands & Eyes Services	3.3.5 Control Activities
Service Level Cross Connect Services	3.3.5 Control Activities
Service Level Cloud Connect Services	3.3.5 Control Activities
Cloud Service Availability	3.3.5 Control Activities
Interxion is committed to maintain industry standard certifications and compliance programs in relevant entities, including ISO27001, ISO22301, SOC2 Type II, PCI-DSS (refer to 3.3.4 – page 26)	3.3.1 Control environment 3.3.2 Communication and Information 3.3.3 Risk Assessment 3.3.4 Monitoring Activities 3.3.5 Control Activities 3.3.6 Logical & Physical Access Control 3.3.7 System Operations 3.3.8 Change Management 3.3.9 Risk Mitigation 3.3.10 Availability

3.1.5 Organisation

Interxion Headquarters is based in the Netherlands and the United Kingdom. Within Interxion Headquarters the departments operate together to provide a central hub and support for the local entities. These departments are:

- **HQ QHSE –** HQ Quality, Health, Safety & Environment
- **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
- **Local entities** – Interxion Netherlands, Denmark, Sweden, United Kingdom, Ireland, Switzerland, Austria and Germany

3.1.5.1 HQ Quality, Health, Safety & Environment (QHSE)

Interxion HQ Quality, Health, Safety & Environment (hereafter HQ QHSE) is responsible for the design, implementation and effective management of Governance, Risk and Compliance within Interxion. It supports the Business, including local entities through a central compliance control framework, operating systems, communication and coordination and organizational structures.

3.1.5.2 HQ 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.

3.1.5.3 HQ HR

Interxion human resources are managed locally and operated within a framework set by the HQ Human Resource department (hereafter HQ HR) 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.

3.1.5.4 HQ European Customer Service Centre (ECSC)

Interxion provides the European Customer Service Centre (hereafter ECSC) as the single point of contact (SPOC) for Interxion customers, 24x365. 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 remote 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 activities. The ECSC is 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 goods deliveries and removals, access authorizations and de-authorizations, 'Remote Hands and Eyes' and cross-connects, 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.

3.1.5.5 Digital Technology & Engineering Group (DT&EG)

The Digital Technology & Engineering Group (DT&EG) team consists of facility experts and 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 Management & Organization matters.

3.1.5.6 Local Entities

Each entity has a dedicated local management team, responsible for Data Centre operations in their respective country. The Managing Director reports to the CEO. The local Quality and Security Managers report to the local organization and functionally to Interxion HQ QHSE.

3.1.6 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 reflects the responsibilities within FRA01, FRA02, FRA03, FRA04, FRA05, FRA06, FRA07, FRA08, FRA09, FRA10, FRA11, FRA12 and FRA13 (hereafter FRA01 - FRA13) and DUS01 - DUS02 locations in Germany. Central Company responsibilities are reflected through the scope of the report and pertain to the following departments; HQ QHSE, HQ ECSC, HQ HR, HQ ICT and DT&EG based between the United Kingdom and the Netherlands.

The local Interxion entities are responsible for compliance to local controls. Interxion Headquarters is responsible for compliance to all central controls. In addition, Interxion Headquarters is coordinating the overall SOC2 program (maintaining the SOC2 framework, progress on compliance (internal and external testing).

3.1.7 External Subservice Organizations

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

3.1.8 Changes to the Control Environment

Interxion has adopted the 2017 Trust Services Criteria (TSP100) and based on the updated Trust Services Criteria Interxion's SOC2 risk assessment and control framework has been reviewed, updated and came to effect as of January 1, 2019. The following changes were caused by the new Trust Services Criteria: Changes in Interxion's SOC2 framework:

- New and updated controls to cover the new Risk management criteria, these new and updated controls contain the following (new) requirements on the risk management process:
    - Controls on the identifying the business objectives and significant changes as input before performing the risk assessment,
    - Identifying and addressing fraud risks,
    - Including external stakeholders and vendors risks and
    - Risk mitigation procedures.
- Inclusion of specific controls on informing and monitoring external stakeholders and vendors criteria affecting the internal control environment.
- Identification, detection, monitoring and preventing vulnerabilities on the configurations, IT infrastructure and applications.
- Entity level controls on the independence and the functioning of the internal control function.

In addition, Interxion has implemented a GRC tool (MetricStream) in 2019. This tool manages internal compliance testing, document control, Enterprise risks and audit management. MetricStream has being rolled-out from the following start date and is implemented in the following phases:

- MetricStream: Compliance: August 31, 2019
- MetricStream: Issue Management: September 30, 2019
- MetricStream Business Impact Analysis: September 30, 2019

The following MetricStream functionalities are scheduled to be implemented:

- MetricStream Audit Management,

To accommodate for future growth and scalability, Interxion started to implement an integrated Service Management platform (ServiceNow) to improve service delivery and efficiency. This Service Management Tool is used for physical security access administration, logging tickets, sending (new) client notifications

and assigning them to the relevant queue. ServiceNow has (partly) replaced Sage CRM during 2019 and is implemented per Interxion entity based on the following (deployment) timelines:

- HQ (incl. ECSC): July 17, 2019
- Germany: September 16, 2019

3.2 Components of the system providing the defined service

Refer to Section IV: Description of Criteria, controls, tests and results of tests for the distinction between local and HQ responsibilities and details of the Trust Services Criteria and Controls

3.2.1 Infrastructure

FRA01 - FRA13 and DUS01 - DUS02 customers can rent rooms, cages and rack space from Interxion Deutschland GmbH. Customers may only access their own space, which is controlled with card access readers and cameras and other methods determined by customers.

The FRA01 - FRA13 and DUS01 - DUS02 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 issues. The facilities offer redundant (N+1) UPS power and redundant (N+1) cooling as well as alarm and monitoring systems. The FRA01 - FRA13 and DUS01 - DUS02 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.

The following critical infrastructure systems are in scope:

- Generators;
- Uninterrupted Power Supplies (UPS);
- CRAC's;
- Chillers;
- Fire detection system;
- Fire suppression system.
- Water leak detection system;

Design Engineering requirements exception fire separation FRA03 and FRA04:

The requirements for the above mentioned infrastructure are formalized and documented in the Design Engineering Requirement managed by DT&EG. As the Design Engineering requirements are used when a data centre is commissioned and as these requirements have significantly changed over time, this means that the older generation Interxion Deutschland GmbH's data centres are no longer fully compliant with the latest Design Engineering Requirements.

To identify the potential risk on the data centre operations of the older (non-compliant) data centre configurations a regular risk analysis is performed by Interxion Deutschland GmbH management. During this risk analysis Interxion Deutschland GmbH management identified that at the FRA03 and FRA04 data centres the setup of the generator room(s) are no longer in accordance with the latest Design Engineering requirements. The generators have no separate fire cells / containments, which can contain a potential fire in order to limit the impact on the operations of the emergency power system of the data centre. In addition in the FRA03 data centre the main fuel tank is placed in the same room as the generators.

Based on the follow-up actions and mitigating measures performed upon the risk analysis, DT&EG management approved an exception to the Design Engineering Requirement for the generator room setup for FRA03 and FRA04. This exception is approved as automatic & passive fire detection systems and manual fire extinguishers are in-place in the generator rooms and as security guards & Interxion Operational employees were trained for manual fire extinguishing (in low risk fire scenarios) and at least two employees (a security guard and/or an on-site engineer) are 24/7 present at the data centres to be able to follow-up on fire detection alarms.

3.2.2 Software

Interxion uses software (on HQ and local level) which are relevant for the security and the availability of their cloud and carrier colocation data centre services to their customers. Interxion uses Customer Relationship Management software (Sage CRM / ServiceNow) 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. Sage CRM, ServiceNow and the Customer portal are managed at HQ and operated by Interxion Deutschland GmbH. Ultimo is used to manage Change Requests and problem management. Critical equipment is monitored by the ECSC and Interxion Deutschland GmbH. 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 Service Management Software 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 Deutschland GmbH the following systems are in scope:

Software	Functionality	Managed
Sage CRM (including Portal)	Platform to manage Customer requests (in progress to be replaced by ServiceNow)	Interxion HQ
ServiceNow (including Customer Portal)	Platform to manage Customer requests	Interxion HQ
MetricStream	Platform to manage Governance, Risk and Compliance	Interxion HQ
Ultimo	Maintenance Planning System	Interxion HQ
BVMS	Bosch Video Management System	Interxion Deutschland GmbH
Jerrasoft	Biometric Control System	Interxion Deutschland GmbH
OPSVIEW	Energy Controlling, Monitoring and Billing System	Interxion Deutschland GmbH
PAC	Access Control System	Interxion Deutschland GmbH
PME	Power Monitoring Expert	Interxion Deutschland GmbH
SOC (Security Operation Center Database)	Database used by security guards for logging security events, visitor and badge details	Interxion Deutschland GmbH
TACVista	Building Management System and cooling monitoring	Interxion Deutschland GmbH
StruxureWare	Building Management System and cooling monitoring	Interxion Deutschland GmbH

3.2.3 People

Interxion Headquarters has a dedicated Operations Support team, which support the local entities in their daily operations. The Managing Directors within the entity have a reporting line to the Group Managing Director. The Operations Managers / Directors have a functional reporting line to the Vice President Operations Support. The organizational charts below show how Interxion Headquarters is organized.

Interxion Deutschland GmbH has a dedicated team assigned for Operations, Customers Services and Infrastructure Management. In the Germany headquarters, local teams support business and operations with Security, Sales & Marketing, Finance, Expansion, Quality, Purchasing and Human Resources departments. Please see the next pages for the high-level organisational charts.

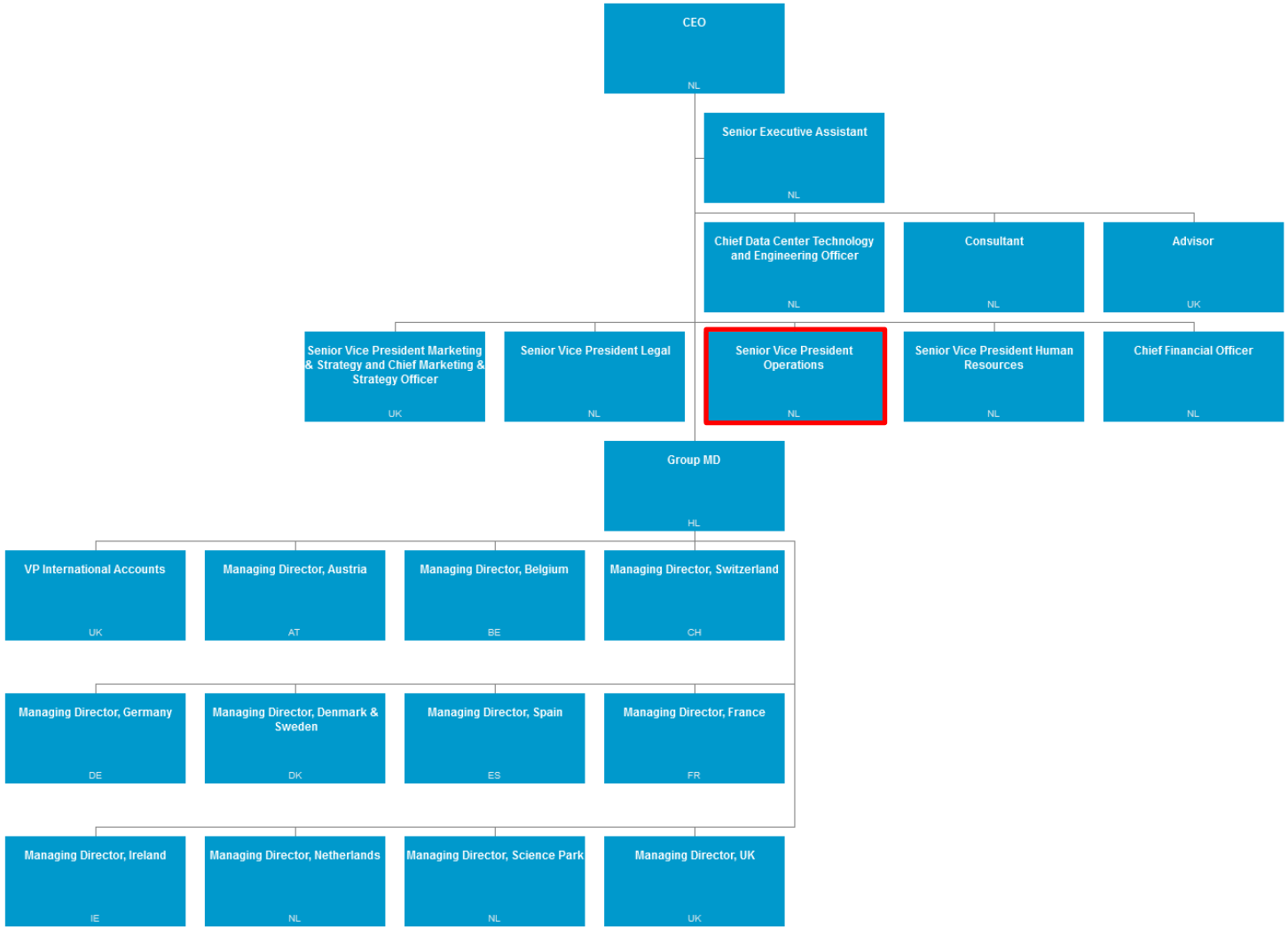


Figure 1a: Organizational structure Interxion Headquarters

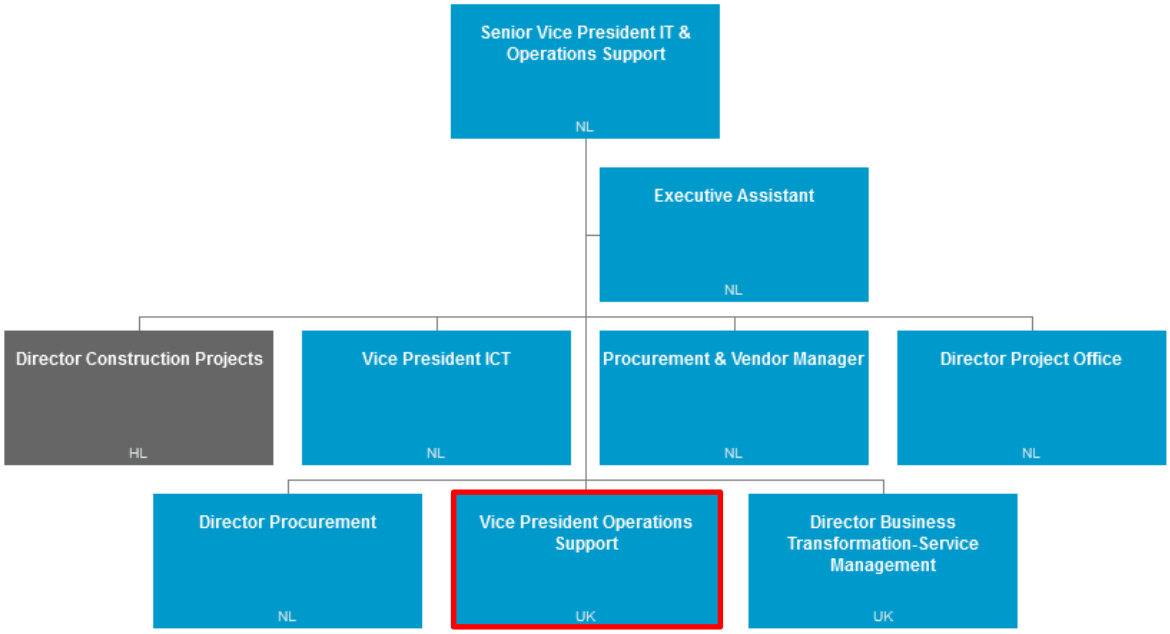


Figure 1b: Organizational structure Interxion Headquarters

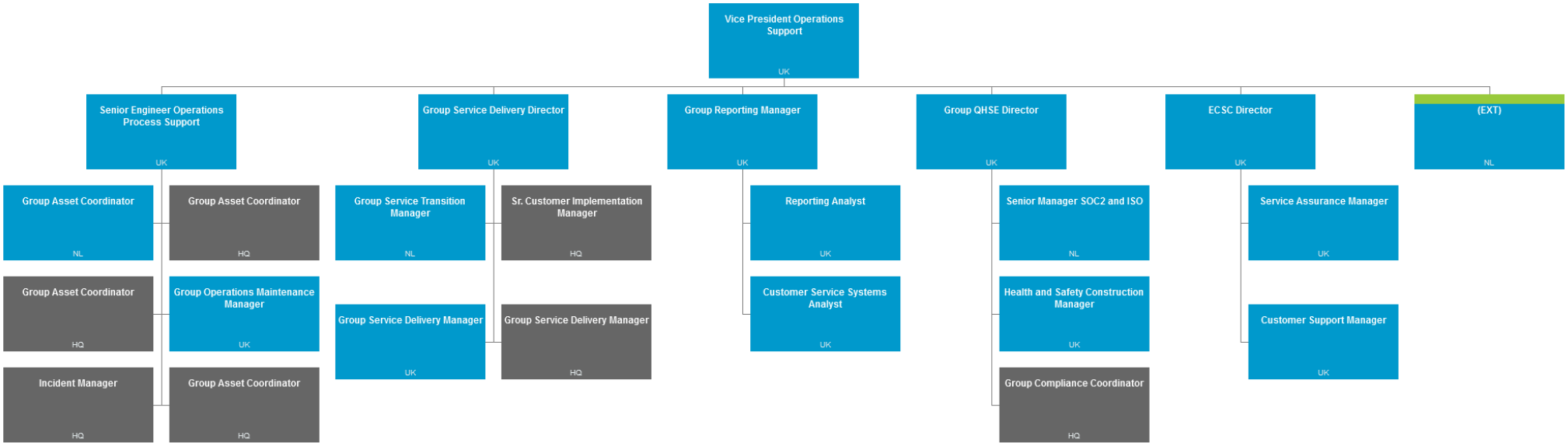


Figure 1c: Organizational structure Interxion Headquarter

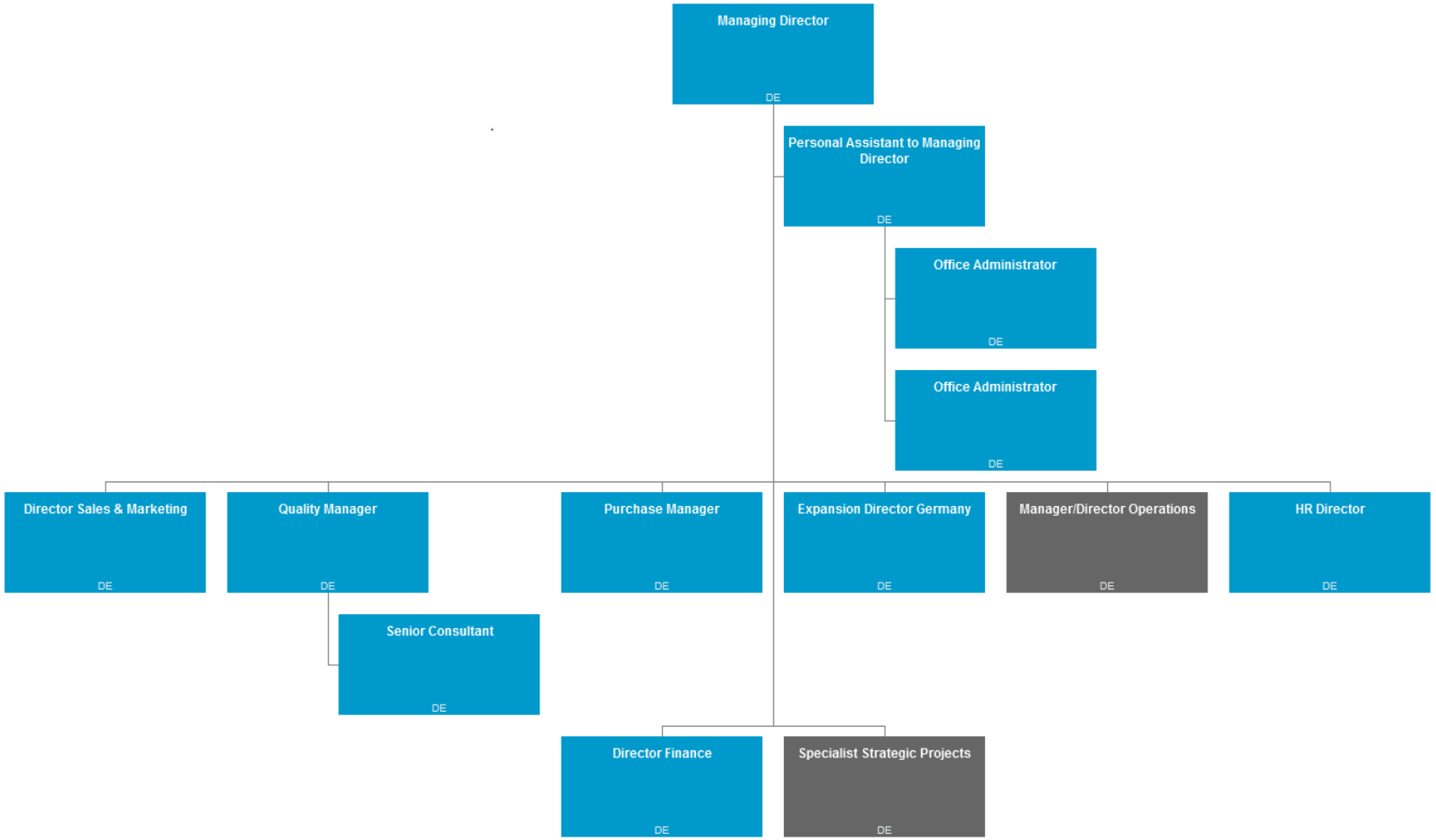


Figure 1d: Organizational structure Interxion Deutschland GmbH

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 in the Document Management System in Interxion's Governance, Risk and Compliance tool.

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 interrelated components of internal control at Interxion:

- **Control Environment**

  The Control Environment demonstrates how Interxion is committed to integrity and ethical values.

  Interxion's board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

  The Control Environment furthermore demonstrates how Interxion's management has established oversight, structures, reporting lines and appropriate authorizations and responsibilities in pursuit of the objectives with the board.

  It demonstrates Interxion's commitment to attract, develop and retain competent individuals in alignment with the objectives. Interxion holds individuals accountable for their internal control responsibilities in the pursuit of the objective.

- **Communication and Information**

  Communication and Information 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. Interxion communicates compliance to internal control information with not only senior management but also appropriate employees and board of directors. Interxion has internal controls around compliance communications with parties external to Interxion and shows compliance to controls inbound from third parties.

- **Risk Assessment**

  Risk Assessment is the process of identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed. Interxion specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Interxion identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. Interxion considers the potential for fraud in assessing risks to the achievement of objectives. Interxion identifies and assesses changes that could significantly impact the system of internal control.

- **Monitoring activities**

  Monitoring Activities are the processes that assess the quality of internal control performance over time. Interxion selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of internal control are present and functioning. Interxion evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

- **Control Activities**

  Control Activities are the policies and procedures that help ensure that management's directives are carried out. Interxion selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Interxion selects and develops general control activities over technology to support the achievement of objectives. Interxion deploys control activities through policies that establish what is expected and procedures that put policies into action.

The supplemental criteria, which apply to the achievement of the entity's objectives relevant to the engagement, are organized as follows:

- **Logical and Physical Access**

  Logical and Physical Access are the processes and systems that manage Physical and Logical Access restrictions. They include how access is granted and revoked and avoids unauthorized access.

- **System Operations**

  Within Interxion, System Operations are the processes and systems which manage, detect and mitigate processing nonconformities, including access (physical and logical) security nonconformities.

- **Change Management**

  Change Management demonstrates how Interxion recognizes the necessity for changes, executes the changes using a controlled process and prevents unauthorized changes from occurring.

- **Risk Mitigation**

  Risk Mitigation within Interxion recognizes, chooses, and advances risk mitigation activities that have occurred from business disruptions, and the monitoring and evaluation of the use of business partners and vendors.

- **Additional criteria for Availability**

  Interxion maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. Interxion authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. Interxion tests recovery plan procedures supporting system recovery to meet its objectives.

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 Organizational Structure

Interxion has a 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.

Interxion GRC Council consists of non-executive directors and acts independently from operational management, represented through the GRC Committee. Oversight responsibilities of Interxion GRC council and committee members, including relevant competence about internal controls, is documented within the Information Security Manual. As required Interxion shall make use of external consultants to supplement the knowledge and expertise of the GRC Council and / or GRC Committee and / or sub-committees.

3.3.1.2 Integrity and ethical values

Interxion is an industry-leading provider of carrier neutral internet data centre services. In order to develop further, 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 remain 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 Code of Conduct and sets out the principles that Interxion, as a company, and as individuals will adhere to. The Code of Conduct also helps the Interxion employees to understand the responsibilities as employees of the Interxion group of companies. To that end, the Code of Conduct 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. Interxion complies to a strictly enforced audit and governance framework, including 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.

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.

3.3.1.4 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 position 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. Third party contractors are responsible for carrying out background checks on staff working at Interxion unless specified in contracts.

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 Communication and Information

3.3.2.1 Internal Communication and Information

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 Director Operations and the Director ECSC 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 also regularly meets to share information in the departments. Regular management reviews are held in order to evaluate Management System efficiency and performance effectiveness.

Interxion regularly communicates 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.

3.3.2.2 External Communication and Information

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). Upon creation of the customer’s account, the identifiable customer point of contact, is provided controlled access to the company customer portal 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 & Safety Rules” within Interxion facilities.

Customers can interact with Interxion by following procedures and processes described through use of 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.

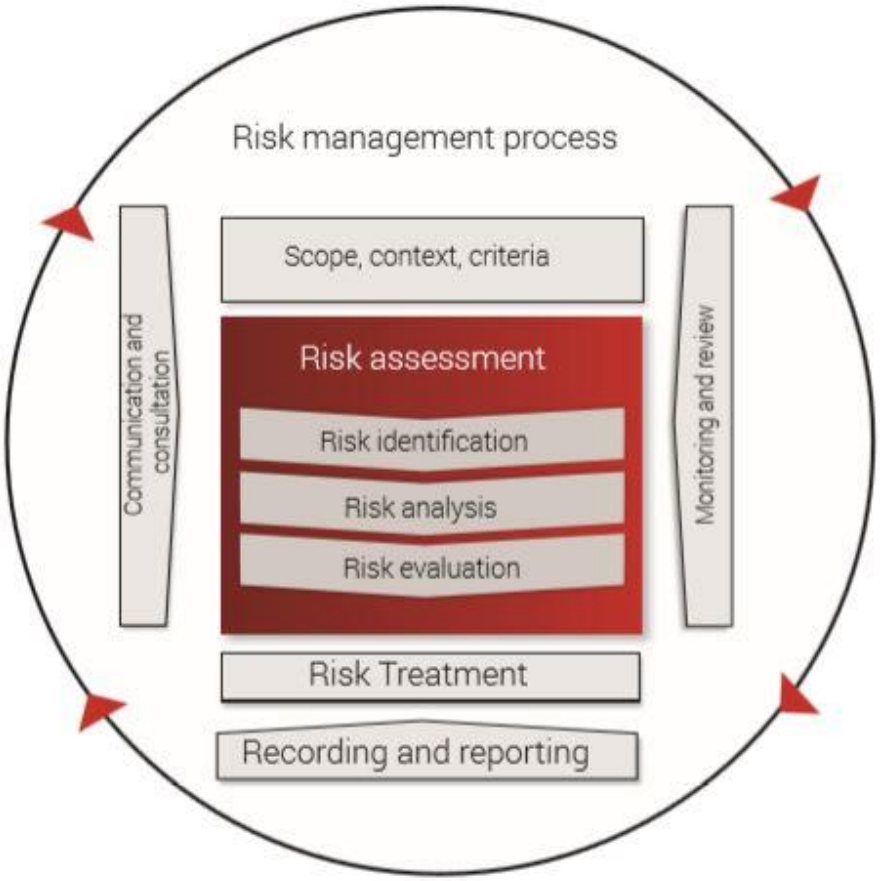
In cases where an unforeseen event occurs such as an incident or the resulting need for an emergency change, the ECSC communicates the progress to resolution and informs customers accordingly, the period of this update is based on the estimated time to fix. During an outage, communication is also established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

Interxion Deutschland GmbH can provide reports to customers and hold regular meetings with customers as a contractual option. For some 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.

3.3.3 Risk Assessment

Interxion follows the ISO 31000 standard to achieve effective risk management and realisation of business objectives. The risk assessments are based on Interxion's business and control objectives that are aligned to the core values "Courage", "Passion", "Teamwork" and "Customer Focus". Interxion considers risk management as a core to creating, maintaining and improving the control environment that results in quality, consistency and control effectiveness. Interxion leadership is committed to apply risk management through the management systems to achieve greater value and efficiency of processes and business assurance. Risks are assessed at HQ level and country level to achieve both consistency and relevance through the organisation and capitalise on awareness and ownership

Interxion's Risk Assessment operates according to ISO 31000 Risk assessment process as below:



Interxion considers risk assessment as a continuous exercise and periodically reviews the assessed risks based on change in the external and internal contexts. Interxion's Quality Management is responsible for identifying and assessing changes that could significantly impact the system of internal controls as part of the risk management procedures. The following changes are considered in the Interxion Risk Management process:

- Changes in the External Environment
- Changes in the Business Model
- Changes in Leadership
- Changes in Systems and Technology
- Changes in Vendor and Business Partner Relationships

Inherent and residual risks are assessed based on the achievement of objectives, the design and effectiveness of controls and the continuous consideration of potential threats. Interxion Risk Management personnel evaluates the risk of fraud within its business and documents the identified fraud risks in the risk register, risk assessment plans and risk assessments. Interxion continuously evaluates the risk of fraud within its business and has documented control processes that are independently attested. Interxion complies to the SOx Control Framework, which includes fraud mitigation measures.

Strategic direction, ambition and momentum is based on risk assessment outputs and supports business maturity and increased shared value with internal and external stakeholders.

3.3.4 Monitoring activities

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 performs internal audits based

around the concept of identifying risks that could inhibit the effectiveness of the controls. Where applicable metrics are generated from KPI's extracted from empirical data, such as the service management and GRC tools in use, to ensure that control processes are functioning as intended. These audits are performed at local level by the Interxion Senior Manager for Quality and Compliance.

Interxion performs an annual assessment of the required (quality) information to support the functioning of the internal control framework. The assessment on internal control information contains a specification of the internal and external sources of data and information systems, and a review by Interxion Quality Management is performed whether the information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.

The internal audits 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 and implemented. Physical Site Security Audit is performed annually to verify the facilities; building, fence, security systems, CCTV, access etc.

A GRC Committee is implemented, having regular meetings. Responsibilities include:

- 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
- Supplier Management Follow up

Network penetration testing is carried out by a trusted third party on an annual basis. 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 as prescribed in the Vulnerability Management procedure.

The allocated 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 live operational environment.
- The asset owners are responsible for tracking likely vulnerabilities in and patches available for their assets.
- High value or high-risk systems are treated ahead of other systems.
- Identified vulnerabilities for organizational assets are classified as priority one and acted upon in an equivalent manner.
- All vulnerabilities are first 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, considering the balance between risks of installing and not installing, before the final decision as to necessary controls can be made.
- External points of contact 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 and 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 is installed on all Interxion workstations, laptops and servers that support this control system. All configuration items are regularly reviewed to ensure they have the latest version of the anti-virus software installed. The software is periodically updated and a report is created to identify and systems found to have earlier software versions installed.

Interxion is continuously reviewing and 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 27001 & ISO 22301 (Annually)
- External audit: ISO 27001 & ISO 22301 (per certification scheme)
- Internal audit: ISO 14001 (Annually)
- External audit: ISO 14001 (Annually)
- Internal audit: ISO 50001 (Annually)
- External audit: ISO 50001 (Annually)
- Internal audit: ISO 9001 (Annually)
- External audit: ISO 9001 (Annually)

- External audit: PCI-DSS (Annually)

3.3.5 Control activities

Interxion's *Control Activities* are the policies and procedures that help ensure that management's directives are carried out.

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 Governance, Risk & Compliance Committee and are almost exclusively owned by the Vice President Operations. The Director QHSE has the mandate to approve policies and procedures. The only exceptions are technical or documents containing information that require specific expertise. These documents are owned 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 reviewed at country level to ensure all entities are fully aware of them and understand them.

All Interxion HQ policies and procedures are reviewed regularly by the HQ Group Senior Compliance Manager. The local policies and procedures are reviewed regularly by the local owner. Local policies and procedures are also reviewed during the various internal audits carried out by both technical (DT&EG) and compliance (HQ Group Senior 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 documented Management System, structure is compliant with the ISO27001:2013 standard.

Document name	Mandate	Country	Type
Risk Management Policy	HQ	Global	Policy
Risk Management Procedure	HQ	Global	Procedure
Interxion Information Security Policy and Manual	HQ	Global	Policy
Information Security Committee	HQ	Global	Policy
Policy Against Malicious Code (malware)	HQ	Global	Policy
Physical Access Security Policy	HQ	Global	Policy
Business Continuity Management Policy	HQ	Global	Policy
Interxion Information Security Compliance Policy	HQ	Global	Policy
Corporate Data Protection & Privacy Policy	HQ	Global	Policy
Acceptable Usage Policy (AUP)	HQ	Global	Policy
Personnel Screening Procedure	HQ	Global	Procedure
Access Control Policy	HQ	Global	Policy
Legal Compliance Data Subject Request policy	HQ	Global	Policy
Onboarding Policy	HQ	Global	Policy
Operational Incident Management Policy	HQ	Global	Policy
Confidentiality Agreements	HQ	Global	Procedure
Inventory & Ownership of Assets	HQ	Global	Procedure
Media and Information Handling Procedure	HQ	Global	Procedure
Versioning & Classification	HQ	Global	Procedure
Documented IT working procedures	HQ	Global	Procedure
Reporting physical and environmental security weaknesses & events	HQ	Global	Procedure

Document name	Mandate	Country	Type
System Planning & Acceptance	HQ	Global	Procedure
Vulnerability Management	HQ	Global	Procedure
Joiner & Leavers Procedure	HQ	Global	Procedure
Remote Access Procedure	HQ	Global	Procedure
Access Control Rules & Rights for Users/User Groups	HQ	Global	Procedure
Backup Procedures	HQ	Global	Procedure
Business Information Systems	HQ	Global	Procedure
Testing, Maintaining & Re-assessing BC Plans	HQ	Global	Procedure
Network Controls & Services	HQ	Global	Procedure
External Parties: Information Security Procedure	HQ	Global	Procedure
Control of Operational Software	HQ	Global	Procedure
Incident Management Processes and Procedures	HQ	Global	Procedure
Information Security Events and Incidents	HQ	Global	Procedure
Change Management Integrated Policy, Process and Procedures	HQ	Global	Procedure
Control of Documents	HQ	Global	Procedure
Retention of Records	HQ	Global	Procedure
Management Review Procedure	HQ	Global	Procedure
Software Installation	HQ	Global	Procedure
Business Continuity Planning	HQ	Global	Procedure
Crisis Management Process and Procedures	HQ	Global	Procedure
Security Surveillance Policy	Local	Germany	Policy
Security Policy	Local	Germany	Policy
Security Service Policy	Local	Germany	Policy
Security Concept	Local	Germany	Policy
Security Access Procedure	Local	Germany	Procedure
Security ID card Policy	Local	Germany	Policy
Security Visitor Policy	Local	Germany	Policy
Security Key Policy		Germany	Policy
Business Continuity Plan	Local	Germany	Policy
De-Man-ICT-LocalApps (Local Application Logical Access Management)	Local	Germany	Procedure

3.3.5.1 Information Security Management

The Interxion senior management team has assigned lead responsibility for information security to the Vice President (VP) Operations Support. 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) as part of the integrated Management System, which details policies and controls that help determine effectiveness of Information Security management. In particular, the ISMS is defined as the part of Interxion Deutschland GmbH 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 Deutschland GmbH. 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 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 Deutschland GmbH has its own Security 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 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.

3.3.5.2 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 may 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 Director Operations is responsible for managing security responses and depending 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 Director 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 Director Operations, who will inform the ECSC in accordance with the Operational Incident Management Procedure. Where customers have assigned a Security contact the incidents shall be reported by the Director 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 Director Operations to the customer Security contact.

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

The events should be reported by the Director 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 Director 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 Director Operations is required to retain a Security event log documenting all events and corrective actions and conclusions. Breaches are typically discussed at Director Operations level in biweekly meetings. 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.

3.3.6 Logical & Physical Access Control

3.3.6.1 Logical Access

In the case of logical access to internal ICT systems all requests for access are managed by logging of a request ticket in the ICT Service Portal (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 provides 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 Director Operations 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 the ICT Service Portal (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 an ICT Service Portal 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.

ICT Service Portal 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.

3.3.6.2 Physical Security

Interxion uses security perimeters and layers 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 FRA01 - FRA13 and DUS01 - DUS02 colocation data centres physical security controls are designed as a "building within a building" and include:

- The data centres FRA01 - FRA13 and DUS01 - DUS02 are permanently secured by security guards that are present 24x365 on site.

  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 90 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 personnel with specific levels of authorisation. The Managing Director is responsible for authorizing access to Interxion areas, and security levels and access are reviewed on a periodic basis. All permanent and temporary physical access rights are managed through the Customer Portal.

3.3.7 System Operations

3.3.7.1 Environmental systems

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.

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 handheld 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.

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.

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.

3.3.7.2 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.

3.3.7.3 Alarm Monitoring

The first response on alarm notifications on security and availability incidents and breaches is a local responsibility. Second line alarm monitoring is performed by Interxion HQ ECSC. Interxion HQ ECSC will follow-up on alarm notifications with Local entity (engineer) whether escalation to an incident is necessary (Interxion HQ responsibility).

Alarms and incidents are analysed thoroughly, and corrective actions are achieved via the Incident Management process and Change Management process. A maintenance window is scheduled to apply any such corrective actions. 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.

3.3.7.4 Incident Management

In case of an incident, an incident coordinator both on site and at the ECSC is appointed, 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 Director Operations, the Service Operations Manager, the Facility Manager, HQ Operations Support and a DT&EG engineer. An incident report, containing a root cause analysis, is provided to any customer that is impacted by a security breach and/or availability (e.g. outage) 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 Director Operations 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.

3.3.8 Change Management

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 to customer services. The change management process follows a structured documented approach and includes notification to involved parties.

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 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 applying the risk assessment approach and respecting greater urgency. 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.

3.3.9 Risk Mitigation

Interxion risk mitigation activities include policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that could disrupt business operations and impact the ability to realise business objectives. Monitoring processes, verification, information and communicating protocols are structured around company and local affecting foreseeable events and disruption.

Financial impact of loss events are offset with insurance policies that would otherwise impair the company objectives to be realised.

3.3.10 Availability – Additional Criteria

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 daily and restores are tested every two months.

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 Criteria 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 Deutschland GmbH 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.

CC6.4: Interxion restricts physical access to facilities and protected information assets (for example, Data Centre facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the Interxion's objectives. &

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

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 the FRA01 - FRA13 and DUS01 - DUS02 data centres only authorized people (registered ID) are present on the ACL.
- Ensuring that access requests to the FRA01 - FRA13 and DUS01 - DUS02 data centres 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 Deutschland GmbH as soon as is practicably possible.
- Ensuring that its employees follow the "House Rules" provided in the contract and posted at the FRA01 - FRA13 and DUS01 - DUS02 data centres' reception desk.
- 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: Interxion authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

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: Interxion maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Client management is responsible for:

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

interxion™

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, Control Activities, Logical and Physical Access Controls, System Operations, Change Management, risk assessment processes, communication and information 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 to Trust Services Criteria Availability);
- Criteria related to the Control Environment (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Communications and Information (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Risk Assessment (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Monitoring Activities (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Control Activities (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Logical and Physical access (applicable to Trust Services Criteria Availability and Security);
- Criteria related to System Operations (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Change Management (applicable to Trust Services Criteria Availability and Security);
- Criteria related to Risk Mitigation (applicable to Trust Services Criteria Availability and Security).

4.4 Criteria related to Availability

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**A1.1 – 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. Refer to CC4.1 - control A	☒		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 Deutschland GmbH's 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 by the country operations team on signing of initial contract and ongoing to 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 was regularly evaluated by the Interxion Deutschland GmbH's operations team. For a sample of new Interxion customers and contract renewals, inspected the ticket documentation and e-mail communication with the Capacity Manager, to determine whether the capacity requirements were evaluated upon signing of the (initial / renewed) contract.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**A1.2 - 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: - 24/365 monitoring of the facility on alarms by both local operations, as well as the ECSC - 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. Inquired of management, observed the data centre and inspected monitoring tooling and alarm documentation to determine whether 24/365 monitoring on power supply related alarms, by local operations, was performed. Inquired of management, observed the ECSC monitoring room and inspected the alarm and ECSC monitoring shift documentation to determine whether 24/365 monitoring on power supply related alarms, by the ECSC, was performed. 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	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**A1.2 - 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 The Design Engineering Requirement is reviewed on a regular 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 the alarm and 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.	Deviations noted. *Interxion Deutschland GmbH:* For two (2) (FRA08 and FRA09) of the fifteen (15) in-scope Interxion Deutschland GmbH's data centres, we determined, per on-site observation that five (5) generators units did not have fire detections systems (or fuel cut-off systems) installed. For FRA09 we determined that none of the three (3) generators present have fire detection systems installed. At FRA08 we determined that two (2) (client specific) generators of the total seven (7) generators at FRA08 did not have fire detection systems installed. Per inquiry with Interxion Deutschland GmbH management we determined that no risk assessment and/or corrective actions on the missing fire detection systems of FRA08 and FRA09 were performed to limit the risk of not having detection systems in the generator containments. The main mitigating factors identified are: - We determined that the generators of the FRA08 and FRA09 data centres are placed in separate fire cells / containments outside the data centre building which limits the potential impact on the operations of the emergency power system in case of a fire in the containment in which the generators are placed.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		Per observation we determined that no other fire detection / suppression measures were in place. - Manual fire suppression systems are located in close proximity to the generators and trained staff is able to respond to small, low risk fire scenarios. No other deviations noted. *Approved exception on the Design Engineering Requirement:* For two (2) (FRA03 and FRA04) of the fifteen (15) in-scope Interxion Deutschland GmbH's data centres, we determined, per onsite observation, that there are no separate fire cells / containments for the generators in-place, which can contain a potential fire in order to limit the impact on the operations of the emergency power system of the data centre. In addition we determined that for one (1) (FRA03) of these data centres also the main fuel tank is placed in the same room as the generators, which increases the risk of an uncontained fire in case fire breaks out in this room. We determined, per inquiry with Interxion management and inspection of the risk assessment documentation that an, by Interxion Deutschland GmbH management and DTEG management approved, exception to the Design Engineering Requirement was available based upon a formal risk analysis.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
						We determined, per observation during the site visit and per inspection of supporting documentation, that automatic and passive fire detection systems were implemented, manual fire extinguishers were present, security guards and Interxion Operational employees were trained for manual fire extinguishing (in low risk fire scenarios) and at least two employees (a security guard and/or an on-site engineer) were 24/7 present at the data centres to be able to follow-up on fire detection alarms.
		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 a regular 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, inspected alarm and ECSC monitoring shift documentation to determine whether 24/365 monitoring on water leakage alarms, by the ECSC, was performed.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					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	
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**A1.2 - 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 and chillers) 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 a regular 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 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	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					centre infrastructure were reviewed on at least an annual basis and signed off by the CEO (Chief Engineering Officer) before release.	
		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. Changes to the back-up schedule are approved by the Director ICT.		☒	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 and critical data centre infrastructure, are in place and based on a documented scheduled plan are tested annually by the entity responsible operations/ITC team 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 Interxion Deutschland GmbH's	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					operations team has tested the Business Continuity procedures at least annually.	

4.5 Criteria related to the Control Environment

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CC1.1 - 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.	☒	☒	Inspected the Code of Conduct and Acceptable Use Policy to determine whether the set of rules outlining the responsibilities and ethics and the statement of confidentiality and privacy practices were defined. For a sample of Interxion employees who were either hired or transferred during the audit period, inspected the compliance report to determine whether new hires or transferred employees have read the Code of Conduct and Acceptable Use Policy and accepted and formally affirmed these responsibilities upon hire or transfer and determined that monitoring by management was performed. For a sample of Interxion employees and contractors with access to organisational information assets, inspected the Code of Conduct refresher course report and 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 annually and determined that monitoring by management was performed.	Deviations noted. *Interxion HQ:* For five (5) out of twenty-five (25) randomly selected Interxion employees and contractors, with access to organisational information assets, we determined through inspection of Acceptable Use Policy (AUP) acceptance list that the AUP reaffirmance has not been completed. We determined per inspection of the Acceptable Use Policy (AUP) and Information Security policy that an updated AUP was released on March 5, 2019 and reaffirmance by all (current) Interxion employees and contractors, with access to organisational information assets, was required. We determined, per inspection of e-mail communication, that follow-up actions were performed for the selected Interxion employees and contractors, however we determined that there was no formal process implemented to enforce completion of the AUP reaffirmance. We determined, per inspection of the control report from the GRC tooling, that a monthly control activity for local HR has been implemented in December 2019 in the GRC tooling which required local HR to follow-up with the respective line manager or

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
						in case of low reaffirmance rates, directly with the employee. We determined that over the period March, 2019 – December, 2019 these control activities did not result in the reaffirmance of the AUP for the five (5) selected Interxion employees and contractors and we were unable to determine that these employees read and accepted the updated requirements in the AUP. No other deviations noted.
		CC1.1 - control B: Hiring procedures include background checks or reference validation, which are performed by HR and retained electronically within the HR application.	☒	☒	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 and retained electronically within the HR application to enable Interxion to meet the security and availability commitments and requirements.	No deviations noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CC1.2 - control A**: Interxion Security Council acts independently from Interxion Operational management and has sufficient members (33% has no direct link to the Interxion Security Committee). Oversight Responsibilities of the Interxion Security board members and Relevant Expertise on the internal controls are documented in the Information Security Manual. If required, Interxion shall make use of external consultants to supplement the knowledge and		☒	Inspected the Information Security Manual, organizational structure diagram and Business Continuity Management policy to determine whether the Interxion Security Council acts independently from Interxion Operational management and has sufficient members of which 33% has no direct link to the Interxion Security Committee. Inquired of management and inspected the Information Security Manual to determine	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		expertise of the Security Council and / or Security Committee and / or Quality / Security Group.			whether the oversight responsibilities of the Interxion Security board members and relevant expertise on the internal controls has been documented. Inquired of management and inspected the assessment on the expertise of the Interxion Security board members to determine whether their knowledge and expertise was evaluated and, if required, external consultants were used to supplement the required knowledge and expertise of the Security Council and / or Security Committee and / or Quality / Security Group.	
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CC1.3 - control A**: Interxion has defined organizational structure, reporting lines, authorities, and responsibilities. These are revised when necessary to help meet changing commitments and requirements. Communication (monthly performance reports and meetings) on the functioning of internal controls exists between Interxion Operational Management and the board of directors so that both have information needed to fulfil their roles with respect to the entity's objectives.	☒	☒	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. For a sample of months, inspected the monthly performance reports and meeting minutes to determine whether the functioning of internal controls was reviewed by Interxion Operational Management and communicated to the board of directors to ensure that Operation management and the board of directors have the information needed to fulfil their roles with respect to the entity's objectives.	No deviations noted.
		CC1.3 - control B: Roles and responsibilities are defined in written job descriptions. The job descriptions are periodically reviewed involving HR and adjusted as needed, which are then electronically stored within the HR application.	☒	☒	Inspected the job matrix and overview of assigned job functions to determine whether assigned job functions are based on job descriptions, which containing	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					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.	
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CC1.4 - control A**: Hiring process is performed in accordance with recruitment policy, which is managed by HR. Candidates suitability for employment includes qualification verification, for professional roles and periodical performance reviews to ensure competences are equal to objectives and role requirements.	☒	☒	Inspected the hiring and transfer procedure to determine whether the candidates' suitability to meet the job requirements was 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' suitability to meet the job requirements was evaluated as part of the hiring or transfer evaluation process.	No deviations noted.
		CC1.4 - 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.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC1.4 – 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.
	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CC1.5 – control A:** Responsibilities and accountability related to the management of internal controls are defined in local and company level policies and procedures.	☒	☒	Inspected relevant in-scope security documentation, availability procedures and other system requirement documentation to determine whether the responsibilities and accountability related to the management of internal controls were defined.	No deviations noted.

4.6 Criteria related to Communications and Information

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**CC2.1 - control A**: Interxion performs an annual assessment of the required (quality) information to support the functioning of the internal control framework. The assessment contains a specification of the internal and external sources of data and information systems, and reviews whether the information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.		☒	Inquired of management and inspected the assessment of the internal control framework and GRC tooling reports to determine whether the annual assessment by Interxion's Quality Management, of the required (quality) information to support the functioning of the internal control, was performed. Inspected the GRC tooling configuration and review evaluation documentation to determine whether the assessment contains a specification of the internal and external sources of data and information systems and reviewed by the Senior Manager for Quality and Compliance whether the information systems produce information that was timely, current, accurate, complete, accessible, protected, verifiable, and retained.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC2.1 – control B: Interxion has defined organizational structure, reporting lines, authorities, and responsibilities. These are revised when necessary to help meet changing commitments and requirements. Communication (monthly performance reports and meetings) on the functioning of internal controls exists between Interxion Operational management and the board of directors so that both have information needed to fulfil their roles with respect to the entity's objectives. Refer to CC1.3 - control A	☒	☒	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. For a sample of months, inspected the monthly performance reports and meeting minutes to determine whether the functioning of internal controls was reviewed by Interxion Operational Management and communicated to the board of directors to ensure that Interxion Operational management and the board of directors have the information needed to fulfil their roles with respect to the entity's objectives.	No deviations noted.
	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CC2.2 – 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.	Deviations noted. Refer to CC1.1 – control A

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
			☒		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.	Deviations noted. *Interxion Deutschland GmbH:* We determined, per inspection of local Information Security Management (ISM) Online Training participation statistics report, that 98 out of the 197 Interxion Deutschland GmbH's employees had not started or completed the annual Information Security Awareness training during the examination period. Per inquiry with Interxion Deutschland GmbH management we were informed that the low participation rate is due to the fact that Interxion Deutschland GmbH did not receive the participation statistics report from Interxion HQ HR in the period from July 2019 until December 2019 and therefore was not able to follow up on those employees who did not yet started of completed their annual Information Security Awareness training. We determined, per inspection of e-mail communication from December 13, 2019, a reminder was sent to Interxion Deutschland GmbH employees to finalize the annual ISM Online Training. No other deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC2.2 – control B: Interxion has clearly defined security and availability responsibilities in the Information Security Manual, which are published to the internal users. In addition, responsibilities have been made specific in the job descriptions and annual objective settings of relevant personnel. The responsibilities and objectives are documented in the HR application.		☒	Inspected the Information Security Manual and 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. Inspected the job descriptions and the configuration of the HR application to determine whether security and availability responsibilities have been made specific in the job descriptions and the annual objectives of operations personnel were documented in the HR application.	No deviations noted.
		CC2.2 – control C: Significant processes are documented in Policies and procedures. This includes responsibility for reporting operational failures, incidents, system problems, concerns, whistle blower 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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CC2.2 – control D:** Interxion has defined organizational structure, reporting lines, authorities, and responsibilities. These are revised when necessary to help meet changing commitments and requirements. Communication (monthly performance reports and meetings) on the functioning of internal controls exists between Interxion Operational management and the board of directors so that both have information needed to fulfil their roles with respect to the entity's objectives. Refer to CC1.3 - control A	☒	☒	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. For a sample of months, inspected the monthly performance reports and meeting minutes to determine whether the functioning of internal controls was reviewed by Interxion Operational Management and communicated to the board of directors to ensure that Interxion Operational management and the board of directors have the information needed to fulfil their roles with respect to the entity's objectives.	No deviations noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CC2.3 - control A:** Interxion informs relevant external stakeholders (contractors, suppliers, service providers) about the internal control environment by communicating Interxion's requirements (House rules and Terms & Conditions for contractors and Non-disclosure agreements (NDA's) for Service Providers). Every entity shall define and document which suppliers are considered 'relevant'.	☒	☒	Inspected the Interxion Corporate Procurement Policy, Supplier policy, House rules and Terms & Conditions for contractors and Non-disclosure agreement (NDA) to determine whether Interxion Deutschland GmbH has defined and documented which suppliers were considered 'relevant' and whether Interxion's requirements and communication to relevant external stakeholders (contractors, suppliers, service providers) were defined. For a sample of contractors, suppliers and service providers, inspected the signed House rules and Terms & Conditions for contractors and Non-disclosure agreements to determine whether Interxion's requirements were communicated and confirmed.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC2.3 - control B: A formally documented system description is communicated to authorized external users via the welcome pack at the time of contract signature or revision as applicable and is made available to internal users on the intranet.	☒	☒	Inspected the introductory welcome pack to determine whether the documents contain key information about the data centre facility responsibilities and contain Interxion's responsibilities to enable customers to carry out their responsibilities. Inspected the intranet website to determine whether the formally documented system description was published and accessible to the internal users. For a sample of new authorized external users, inspected the communication of the introductory welcome pack, to determine whether the welcome pack was communicated to the customer at the time of contract signature or revision as applicable.	No deviations noted.
		CC2.3 - control C: 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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC2.3 - control D: 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.

4.7 Criteria related to Risk Assessment

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CC3.1 – control A**: Interxion's company objectives are reviewed once a year by Senior Management and are included in the risk assessment register and assessment plans. Interxion's Risk Management personnel review the company objectives on their impact on the risk management process and if necessary, implement changes to the risk assessment process and documentation.		☒	Inspected the Interxion's company objectives, risk management procedures and GRC tooling to determine whether company objectives were defined and included in the risk assessment register. Inquired of management and inspected Interxion's company objectives and review documentation to determine whether the annual review on the company objectives by Senior Management has been performed. Inspected the annual risk assessments, based on the risk management template and the GRC tooling, to determine whether Interxion's Risk Management personnel have reviewed the impact of the company objectives on the risk management process and if necessary, implemented changes to the risk assessment process and documentation.	No deviations noted.
		CC3.1 – control B: 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.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the	**CC3.2 – 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	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	risks should be managed.				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.	
		CC3.2 - 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 Deutschland GmbH management.	No deviations noted.
		CC3.2 - 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. Refer to CC3.1 - control B	☒	☒	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.
		CC3.2 – 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	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**CC3.3 - control A**: Interxion Risk Management personnel evaluates the risk of fraud within its business and documents the identified fraud risks in the risk register, risk assessment plans and risk assessments. Interxion will continue to evaluate the risk of fraud within its business and have documented control processes that are independently attested. Interxion will continue to comply to the SOx Control Framework, which includes fraud mitigation measures. Fraud risks are included in the risk register, risk assessment plans and risk assessments.		☒	Inspected the risk management procedures and the Anti-Fraud program to determine whether the risk of fraud within its business and documents was identified in the risk register, risk assessment plans and risk assessments. Inquired of management and inspected Anti-Fraud risk assessment, the SOx Control Framework and GRC tooling to determine whether risk of fraud and fraud mitigation measures were documented in control processes and independently attested.	No deviations noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CC3.4 - control A**: Interxion's Quality Management are responsible for identifying and assessing changes that could significantly impact the system of internal controls as part of the risk management procedures. The following changes are considered in the Interxion Risk Management process: - Changes in the External Environment - Changes in the Business Model - Changes in Leadership - Changes in Systems and Technology - Changes in Vendor and Business Partner Relationships	☒	☒	Inquired of Interxion's Quality Management and inspected risk management procedures to determine whether the assessment of changes that could significantly impact the system of internal controls as part of the risk management procedures was defined. Inspected the risk management procedures and annual risk assessments to determine whether changes in External Environment, Business Model, Leadership, Systems and Technology, Vendor and Business Partner Relationships were considered in the Interxion Risk Management process.	No deviations noted.

4.8 Criteria related to Monitoring Activities

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CC4.1 - 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 Deutschland GmbH's 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. Refer to CC7.2- control A		☒	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 days, inspected the daily guard reports containing the security and availability alarms of the environmental protection systems in the data centre, inspected the incident ticket and e-mail	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					communication, to determine whether the appropriate follow-up has been taken, including customer communication notification (if appropriate).	
		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 by an approved external party. Any issues identified are evaluated by HQ ICT and follow-up actions are documented in a controlled environment under the responsibility of HQ ICT.		☒	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.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the	**CC4.2 - 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. Refer to CC4.1 - control A	☒		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 Deutschland GmbH's Operational Management.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	board of directors, as appropriate.	**CC4.2 - control B**: Interxion has defined organizational structure, reporting lines, authorities, and responsibilities. These are revised when necessary to help meet changing commitments and requirements. Communication (monthly performance reports and meetings) on the functioning of internal controls exists between Interxion Operational management and the board of directors so that both have information needed to fulfil their roles with respect to the entity's objectives. Refer to CC1.3 - control A	☒	☒	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. For a sample of months, inspected the monthly performance reports and meeting minutes to determine whether the functioning of internal controls was reviewed by Interxion Operational Management and communicated to the board of directors to ensure that Interxion Operational management and the board of directors have the information needed to fulfil their roles with respect to the entity's objectives.	No deviations noted.
		CC4.2 - 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. Refer to CC4.1 - control C		☒	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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC4.2 - control D: On an annual basis a penetration test is performed by an approved external party. Any issues identified are evaluated by HQ ICT and follow-up actions are documented in a controlled environment under the responsibility of HQ ICT. Refer to CC4.1 - control D		☒	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 Criteria related to Control Activities

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CC5.1 - control A**: Interxion's Security Council performs 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 the group by the Quality & Security Meeting.		☒	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 and when required updates to Security and Availability policies and procedures were initiated. 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 has been performed in the annual Quality & Security Meeting.	No deviations noted.
		CC5.1 – control B: Vulnerability scans on physical (annual audits are performed on physical security at data centres) and logical (penetration tests) access level are performed at least annually.	☒		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	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					physical access level (physical security audit) has been performed.	
				☒	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. Inspected the annual penetration test and the annual performed security review to determine whether vulnerability scans on logical access level have been performed.	No deviations noted.
		CC5.1 - 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. Refer to CC3.2 – control A	☒	☒	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.
		CC5.1 - 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. Refer to CC3.1 – control B	☒	☒	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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CC5.2 – control A**: Interxion's Security Council performs 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 the group by the Quality & Security Meeting. Refer to CC5.1 - Control A		☒	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 and when required updates to Security and Availability policies and procedures were initiated. 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 the group by the annual Quality & Security Meeting.	No deviations noted.
		CC5.2 – control B: Vulnerability scans on physical (annual audits are performed on physical security at data centres) and logical (penetration tests) access level are performed at least annually. Refer to CC5.1 - Control B	☒		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	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
				☒	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. Inspected the annual penetration test and the annual performed security review to determine whether vulnerability scans on logical access level have been performed.	No deviations noted.
		CC5.2 – 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. Refer to CC3.2 – control A	☒	☒	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.
		CC5.2 – 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. Refer to CC3.1 – control B	☒	☒	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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CC5.3 – control A**: Responsibilities and accountability are defined in the security, availability and other system requirement documentation. Refer to CC1.5 - control A			Inspected relevant in-scope security documentation, availability procedures and other system requirement documentation to determine whether the responsibilities and accountability related to the management of internal controls were defined.	No deviations noted.
		CC5.3 – control B: Interxion has clearly defined security and availability responsibilities in e.g. the Information Security Manual, which are published to the internal users. In addition, responsibilities have been made specific in the job descriptions and annual objective settings of relevant personnel. The responsibilities and objectives are documented in the HR application. Refer to CC2.2 - control B		☒	Inspected the Information Security Manual and 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. Inspected the job descriptions and the configuration of the HR application to determine whether security and availability responsibilities have been made specific in the job descriptions and the annual objectives of operations personnel were documented in the HR application.	No deviations noted.
		CC5.3 – control C: Significant processes are documented in Policies and procedures. This includes responsibility for reporting operational failures, incidents, system problems, concerns, whistle blower and user complaints (and the process for doing so) are published and available on the intranet. Refer to CC2.2 - control C	☒	☒	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.
		CC5.3 – control D: Interxion's Security Council performs annually reviews and approves the Interxion Security and Availability policies and procedures.		☒	Inquired of management to determine whether the security and availability policies and procedures were reviewed	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		Interxion has published it to employees and shall do so to relevant external parties on request. Local consultation is carried out within the group by the Quality & Security Meeting. Refer to CC5.1 - control A			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 and when required updates to Security and Availability policies and procedures were initiated. 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 the group by the annual Quality & Security Meeting.	

4.10 Criteria related to Logical and Physical Access

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**CC6.1 - control A**: Infrastructure components and software are required to be implemented with password submission and separate user ID.	☒	☒	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.
		CC6.1 - 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. Refer to CC6.3 – control B	☒	☒	Inspected authorization listings and authorization matrices to determine whether authorizations were assigned and enforced by the access control system. For a sample of granted / modified access for internal and external users during the audit period, inspected the supporting documentation to determine whether role-based authorizations were assigned in accordance with the logical access procedure.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC6.1 - control C: External points of connectivity are protected by a firewall complex and an Intrusion Prevention System. Refer to CC6.6 – control A		☒	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.
		CC6.1 - control D: 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 application generic accounts are in place if required. Two factor authentication is used for external access to the Interxion network. In case generic accounts are required, mitigating measures (regular account review, password resets and/or password management tooling) are defined and implemented.	☒	☒	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 logical access procedures, account review documentation and supporting documentation on use of exception forms to determine whether the mitigating measures were defined and implemented to ensure the use of generic accounts was limited to only 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.	Deviations noted. *Interxion Deutschland GmbH:* For eight (8) of the eight (8) local applications in scope, we determined that not all accounts have an unique identifier and are not for personal and sole use. Per inquiry with Interxion Deutschland GmbH's Security Manager we determined that no (specific) logical access procedure was defined for the period July until November 2019 on the mitigating measures (regular account review, password resets and/or password management tooling) to limit the risk of using generic accounts. However, we determined that as of December 2019 the following mitigating measures were defined and implemented to prevent unauthorized access to generic accounts: - For all generic accounts, exception forms were in place that specified the reasons for having these accounts and compensating controls were implemented (e.g. password changes). - For access to security applications, physical access is

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		required to the security guard area, which is restricted by physical access controls. - Single sign-on is implemented for three (3) of the eight (8) applications. This ensures that users of the generic accounts are uniquely identifiable by their network account . - Access to generic accounts is controlled by the local application review (refer to CC6.2 – control B/CC6.3 – control A). No other deviations noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**CC6.2 - 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 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 / modified access for internal and external users as created 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 during the audit period, inspected the supporting documentation to determine whether the request was recorded and access was revoked for in scope systems.	Deviations noted. *Interxion Deutschland GmbH*: We determined, per inquiry with Interxion Deutschland GmbH management, that there was no formal user registration and de-registration procedure in place for granting and revoking access to accounts with access to the local applications during the period July, 2019 to November, 2019. Per inspection of the Local Application Management policy we determined that the formal policy, on the registration and de-registration of authorizations to the applications managed by Interxion Deutschland GmbH (local applications), was released and implemented on December 2, 2019. Per inquiry with Interxion Deutschland GmbH management we determined that, prior to the

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		implementation of the formal user registration procedure, the granted and modified access to the local applications was also requested and approved by means of an e-mail or an HR Joiner form sent to the application owner, which deviates from the Interxion HQ Joiner & Leaver procedure that requires the use of an application access form. *User registration:* For two (2) of the five (5) randomly selected granted / modified access to local applications for internal and external users, we determined that no approved application access request form was available. Per inquiry with Interxion Deutschland GmbH management, we determined that the formal user registration procedure was not yet available and implemented at the time the access was assigned. Therefore no application access request form was used to request and approve the access to the local applications. We determined, per inspection of the HR Joiner form and user review documentation of December, 2019, that for both users the granted access was authorized and in line with the job functions of the users. *Interxion HQ ECSC*: For three (3) out of eight (8) randomly selected granted / modified access to Sage CRM for

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		internal and external users, we determined, per inspection of the system generated overview with Sage CRM authorizations and per inquiry with Interxion management, that the user registration process was not followed as no appropriate approval was given (at the time of granting the authorizations) by either the line manager or the application manager. - For one (1) out of these three (3), we determined per inquiry with Interxion management that no authorization request was recorded and no approval by appropriate management was available. As such, we are not able to determine that the formal user registration process was followed. We did obtain screen prints from HQ ICT containing the approval flow of an application request for this Interxion ECSC employee was available, however these screen prints only show the request and approval for access to another application not the authorizations for Sage CRM. - For one (1) out of these three (3), we determined through inspection of the Service Now ticket that the account request was rejected. Nevertheless, we determined, per inspection of the system generated overview with Sage CRM authorizations, that a Sage CRM account was created on May 24, 2019. As such, we determined that

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
						the user registration process was not followed. Based upon our finding we determined per inspection of the account logging that the account was disabled on October 22, 2019 and was never used. - For one (1) out of these three (3), we determined per inspection of the Sage CRM request ticket that a Sage CRM account was not appropriately approved by an authorized approver (line-manager). Per inquiry with Interxion Management, we were informed that due to holiday of the line-manager (authorized approver), access was requested by a direct colleague on August 15, 2019, after which the account was created by ECSC. As such, we determined that the user registration process was not followed. Per inspection of the line-manager approval email that was sent on November 14, 2019, we determined that the Sage CRM account was approved by the line-manager three months after account creation. No other deviations noted.
		CC6.2 - control B: 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. Refer to CC6.3 - control A	☒	☒	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	Deviations noted. Refer to CC6.3 - control A

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					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 whether 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.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**CC6.3 - 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 whether 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.
		CC6.3 - 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 to specific roles for in scope systems.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					For a sample of granted / modified access for internal and external users during the audit period, inspected the supporting documentation to determine whether role-based authorizations were assigned in accordance with the logical access procedure.	
		CC6.3 - 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. Refer to CC6.2 - control A	☒	☒	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 / modified 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.	Deviations noted. Refer to CC6.2 – control A.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**CC6.4 - 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 and temporary contractors, inspected the Sage CRM/ ServiceNow request ticket, visitor log and	Deviations noted. *Interxion Deutschland GmbH:* <u>Assignment badge access rights by Access Groups:</u> We determined, per inquiry with Interxion Deutschland GmbH management and per inspection of the badge access rights, that the granted temporary and permanent physical access rights on customer or contractor role level did not match the requested access rights as specified in the access requests from the Customer Portal /ServiceNow applications.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					badge access log to determine whether the request was recorded and authorized by the access authorizer using the Customer Portal, for the granted access, was available and in accordance with the formal procedures.	Per inspection of the badge access rights assigned and the access request tickets, we determined that physical access rights were granted by assigning Access Groups (related to customer or contractor role) to an access badge, without limiting the access authorizations to the requested on room/cabinet level. We determined, per inspection of the Access groups profiles in the badge system and per inquiry with the Security Manager, that unless agreed differently with the customer, an Access Groups contains all rooms/cabinets related to a certain customer or contractor role, and as the badge access system does not allow for assigning specific authorizations, only pre-configured Access Group profiles can be assigned for the temporary and permanent access requests to the data centre areas. We determined that due to this setup (and limitations) of the badge access system, the granted access rights were not limited to the requested areas, and therefore not in accordance with the central physical security procedure (managed by ECSC) using the Customer Portal/ ServiceNow, which suggests to the (customer) Change List Authorizers (CLA) that they can restrict access on room- and cabinet level.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		Per inquiry with Interxion Deutschland GmbH management, we determined that customers are not (directly) informed about this deviating process by granting Access Groups instead of granting access on room- and cabinet level. <u>Access requests, for visiting customers and temporary contractors</u>*:* For twelve (12) of the twenty-five (25) randomly selected access requests, for visiting customers and temporary contractors, we determined that the name of the Access Group(s) granted matched with the Company Name of the requester. However, we determined that by assigning Access Groups, more customer areas (rooms/ cabinets) were granted than requested. As such, we determined that unauthorized access (to other - not requested - customer areas) was granted. For four (4) of the twenty-five (25) randomly selected access requests, for visiting customers and temporary contractors, we determined that the granted authorizations did not match with the authorizations requested. We did not obtain supporting documentation to confirm whether the additional access rights were formally requested. As such, we could not

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
						determine whether unauthorized access was granted. No other deviations noted.
		CC6.4 - 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.
		CC6.4 - control C: For Customers: all new, changed or revoked permanent physical access rights are requested by a Customer Change List Authorizer, using a central process managed by Interxion's European Customer Service Centre (ECSC). Access requests are processed according to Customer Change List Authorizer credentials and parameters and assigned to Interxion Security at the specific data centre. For Interxion employees: All new, changed or revoked permanent physical access rights are requested by an Interxion Change List Authorizer, using a central process managed by Interxion's European Customer Service Centre (ECSC). Access is validated and granted by the local Security Manager.	☒	☒	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. Inspected the physical security policies and procedures and configuration of Customer Portal and Sage CRM/ ServiceNow to determine whether the central permanent physical access rights requests (new, changed or revoked) process managed by Interxion's European Customer Service Centre (ECSC) was defined and implemented.	Deviations noted. *Interxion Deutschland GmbH:* <u>Assignment badge access rights by Access Groups:</u> Refer to CC6.4 – control A. <u>Granted/changed physical access</u>: For eight (8) of the nine (9) randomly selected granted and changed permanent physical access rights, we determined per inspection of the badge access system access rights and the access ticket that the granted access authorizations (by using pre-configured) Access Groups did not

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					For a sample of granted and changed permanent physical access rights, inspected the Sage CRM/ ServiceNow request ticket submitted by the Customer's or Interxion's Change List Authorizer and badge access logs to determine whether the permanent physical access request was recorded, validated by the local Security Manager (for Interxion employees) and processed in accordance with the physical access rights (credentials and parameters) requested by the Customer's or Interxion's Change List Authorizer and assigned to Interxion Security at the specific data centre. For a sample of requests to revoke permanent physical access, inspected the Sage CRM/ ServiceNow request ticket submitted by the customer's or Interxion's Change List Authorizer, notification to the security guards and badge access logs to determine whether the permanent access to the data centre was timely revoked and processed in accordance with revocation request by the Customer's or Interxion's Change List Authorizer and assigned to Interxion Security at the specific data centre.	match (the more restrictive) access authorizations requested by the customer's CLA. Per inspection of the assigned access rights and the access ticket, we determined that the name of the Access Group(s) granted matched with the Company profile of the person and therefore the access was limited to the customer areas as defined in the Access Group authorizations. For one (1) of the nine (9) randomly selected granted and changed permanent physical access rights we determined that physical permanent access rights to the data centre were granted 9 days before access was formally requested and approved in accordance to the central physical security procedure for managing access. Per inspection of the access request ticket in ServiceNow, we determined that the formal request was created on July 10, 2019 which is 9 days after the access rights were granted to the badge (July 1, 2019). We determined, per inspection of the HR Joiner form and per inquiry with Interxion Deutschland GmbH Management, that access rights were granted based upon the HR Joiner form dated June 17, 2019. No other deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC6.4 - 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.
		CC6.4 - 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.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**CC6.5 - 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. Refer to CC6.4 - control A	☒	☒	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 and temporary contractors, inspected the Sage CRM/ ServiceNow request ticket, visitor log and badge access log to determine whether the request was recorded and authorized by the access authorizer using the Customer Portal, for the granted access, was available and in accordance with the formal procedures.	Deviations noted. Refer to CC6.4 – control A.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC6.5 - 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. Refer to CC6.4 - control B	☒		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.
		CC6.5 - control C: For Customers: all new, changed or revoked permanent physical access rights are requested by a Customer Change List Authorizer, using a central process managed by Interxion's European Customer Service Centre (ECSC). Access requests are processed according to Customer Change List Authorizer credentials and parameters and assigned to Interxion Security at the specific data centre. For Interxion employees: All new, changed or revoked permanent physical access rights are requested by an Interxion Change List Authorizer, using a central process managed by Interxion's European Customer Service Centre (ECSC). Access is validated and granted by the local Security Manager. Refer to CC6.4 - control C	☒	☒	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. Inspected the physical security policies and procedures and configuration of Customer Portal and Sage CRM/ ServiceNow to determine whether permanent physical access rights requests (new, changed or revoked) were processed according to Customer Change List Authorizer credentials and parameters and assigned to Interxion Security at the specific data centre. For a sample of granted and changed permanent physical access rights, inspected the Sage CRM/ ServiceNow request ticket submitted by the Customer's	Deviations noted. Refer to CC6.4 – control C.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					or Interxion's Change List Authorizer and badge access logs to determine whether the permanent physical access request was recorded, validated by the local Security Manager (for Interxion employees) and processed in accordance with the physical access rights (credentials and parameters) requested by the Customer's or Interxion's Change List Authorizer and assigned to Interxion Security at the specific data centre. For a sample of requests to revoke permanent physical access, inspected the Sage CRM/ ServiceNow request ticket submitted by the customer's or Interxion's Change List Authorizer, notification to the security guards and badge access logs to determine whether the permanent access to the data centre was timely revoked and processed in accordance with revocation request by the Customer's or Interxion's Change List Authorizer and assigned to Interxion Security at the specific data centre.	
		CC6.5 - 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). Refer to CC6.4 - control D	☒		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.
		CC6.5 - control E: The sharing of access badges and tailgating are prohibited by policy. Refer to CC6.4 - control E	☒		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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CC6.6 - 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.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**CC6.7 - 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.
		CC6.7 - control B: 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 application generic accounts are in place if required. Two factor authentication is used for external access to the Interxion network. In case generic accounts are required, mitigating measures (regular account review, password resets and/or password management tooling) are defined and implemented Refer to CC6.1 - control D	☒	☒	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 logical access procedures, account review documentation and supporting documentation on use of exception forms to determine whether the mitigating measures were defined and implemented to ensure the use of generic accounts was limited to only authorized personnel. Inspected authentication tools and observed the use of two factor	Deviations noted. Refer to CC6.1 – control D.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					authentication to determine whether two-factor authentication is used for external access to the Interxion network.	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	**CC6.8 - control A**: Anti-virus software is installed on workstations, laptops, and servers 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.

4.11 Criteria related to System Operations

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**CC7.1 - control A**: Interxion performs a monthly scan on the configuration settings of the critical applications and monitoring systems in order to detect vulnerabilities and unauthorized changes. In case vulnerabilities are detected corrective actions are initiated and followed-up by creating an incident ticket.		☒	Inspected the policies and procedures regarding scanning and monitoring on vulnerabilities and unauthorized changes to determine whether the configuration settings of the vulnerability scan tooling, the critical applications and systems and process on initiating and tracking corrective actions was defined. Inspected the configuration settings of the vulnerability scan tooling to determine whether the settings of the scan and monitoring application was implemented in accordance with the defined configuration settings For a sample of months inspected the vulnerability scan reports, evaluation reports and incident tickets to determine whether a monthly scan, to detect vulnerabilities and unauthorized changes to the defined critical applications and monitoring systems, and determined that in case vulnerabilities and/or unauthorized changes were detected the appropriate follow-up was performed and documented in incident tickets.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC7.1 - control B: All critical systems are configured according to documented baselines. Interxion performs an annual scan on these systems. In case unauthorized changes are detected, corrective actions are initiated and followed-up through the (automated) creation of an incident ticket.	☒		Inspected the baseline for configuration settings for critical systems and policies and procedures on the baseline scan to determine whether the security baseline requirements, scope of the critical systems and process to follow-up nonconformities was defined. Inspected the configuration settings of the baseline scan tooling to determine whether the settings of the scan and monitoring application were implemented in accordance with the defined baseline for configuration settings for critical systems and the scope of critical systems. Inspected the annual security baseline scan results report, overview of the scanned systems and incident tickets to determine whether a scan on configuration of critical systems has been performed annually and in case unauthorized changes were detected, determined whether corrective actions were initiated and followed-up through the (automated) creation of an incident ticket.	No deviations noted.
		CC7.1 - control C: Access to the critical data centre infrastructure (security and environmental protection systems) configuration settings is limited to only authorized Interxion personnel by having logical and physical access measures in place in order to prevent unauthorized configuration changes and vulnerabilities. The logical access to the critical infrastructure configurations is limited by having a role-based access group that limit the logical access to system and infrastructure components settings that is enforced by (local) firewall rules.		☒	Inspected the relevant logical access policies and procedures to determine whether logical access measures to limit access to the critical data centre infrastructure (security and environmental protection systems) was defined. Inspected firewall rule procedure documentation to determine whether the firewall configuration settings and role-based access group structure were defined to ensure the logical access to the critical infrastructure configurations was limited.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		The physical access to the critical infrastructure configurations is limited by having a formal role-based access controls that limit the physical access to system and infrastructure components are created and these are enforced by the badge access control system.			Inspected firewall settings to determine whether only the role-based access groups, with the authorized Interxion personnel, were granted access to the data centre infrastructure (security and environmental protection systems).	
			☒		Inspected the relevant physical access policies and procedures to determine whether physical access measures limit access to the critical data centre infrastructure (security and environmental protection systems) was defined. Inspected the badge access system, Sage CRM/ ServiceNow physical access authorizations and physical access review documentation to determine whether the physical access to the data centre areas which contain the critical infrastructure was granted to only authorized Interxion personnel.	No deviations noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.	**CC7.2 - 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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
			☒		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 days, inspected the daily guard reports containing the 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 deviation noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**CC7.3 - 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 escalating 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 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 were responsible for evaluating the impact of logical security and availability breaches and incidents.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					For a sample of logical security and availability alarms of the in-scope IT systems, inspected the ServiceNow 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	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					determine whether the defined protocol has been followed for physical security and availability breaches and incidents.	
		CC7.3 - 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 Deutschland GmbH's operations and security group meetings to determine whether the resolution of security and availability breaches and incidents were reviewed and discussed.	No deviations noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**CC7.4 - 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 escalating security and availability breaches and incidents. Refer to CC7.3 - control A		☒	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 were responsible for evaluating the impact of logical security and availability breaches and incidents.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					For a sample of logical security and availability alarms of the in-scope IT systems, inspected the ServiceNow 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	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					been followed for physical security and availability breaches and incidents.	
		CC7.4 - 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. Refer to CC7.3 - control B		☒	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 Deutschland GmbH's operations and security group meetings to determine whether the resolution of security and availability breaches and incidents were reviewed and discussed.	No deviations noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	**CC7.5 - control A**: Interxion Operational management has documented and implemented the activities to recover from security and availability breaches and incidents in the Business Continuity procedures and Crisis Resolution procedures which are tested annually to restore the functionality in case of a disaster.	☒	☒	Inquired of Interxion Operational Management and inspected the Business Continuity procedures and Crisis Resolution procedures to determine whether the activities to recover from security and availability breaches and incidents are documented and implemented. Inspected the annual Business Continuity test report, of the critical environmental protections systems in the data centre, to determine Interxion Deutschland GmbH has tested the Business Continuity procedures at least annually.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC7.5 - control B: 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 escalating security and availability breaches and incidents. Refer to CC7.3 - control A		☒	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 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 ServiceNow 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.	No deviations noted.
			☒		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.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					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.	

4.12 Criteria related to Change Management

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**CC8.1 - control A:** Changes to the data centre that impact the client, 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 Deutschland GmbH's engineer to determine whether the change was tested before implementation in accordance with Interxion change management procedures.	No deviations noted.
		CC8.1 - control B: 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.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		CC8.1 - control C: 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.	*Interxion HQ ICT:* No occurrence(s): We determined, per inspection of the HQ ICT risk assessment and the HQ ICT planning and budgeting process documentation and per inquiry with Interxion HQ ICT management, that there were no IT infrastructure, data and software projects during the period of examination. As a result, conditions required for the operation of the control did not occur. Therefore, we performed only design testing and no operating effectiveness testing for this control.
			☒		Inspected the Interxion Deutschland GmbH's 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 Deutschland GmbH's project to determine whether change requests and / or business cases were created for the identified and required changes.	No deviations noted.
		CC8.1 - control D: 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.

4.13 Criteria related to Risk Mitigation

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CC9.1 - control A**: Interxion's Risk Management personnel identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Mitigating measures are included in the Business Recovery plan.	☒		Inquired of management to determine whether Risk Management personnel identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Inspected the annual risk assessments, based on the risk management template, to determine whether risks arising from potential business disruptions were evaluated by the Senior Manager for Quality and Compliance based on identified threats and risk tolerances and to determine whether measures were specified to address the identified risks. Inspected the Business Continuity procedures and Crisis Resolution procedures to determine whether mitigating measures risks, arising from potential business disruptions, were documented and implemented in the Business Recovery plan.	No deviations noted.
		CC9.1 - control B: 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. Refer to CC3.2 - Control A	☒	☒	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	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					tolerances and to determine whether measures were specified.	
		CC9.1 - control C: A business recovery plan is in place for each data centre and is reviewed annually by local management. Refer to CC3.2 - Control B	☒		Inspected the business recovery plans for the data centres in scope to determine whether the procedure was in place and annually reviewed by Interxion Deutschland GmbH management.	No deviations noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	**CC9.2 - control A**: Interxion's Risk Management personnel identifies, selects, and develops mitigations on identified risks associated with vendors and business partners through an enterprise risk management system and with GDPR and IT Security surveys and is documented in the risk register, risk assessment plans and risk assessments.		☒	Inquired of management to determine whether Risk Management personnel identifies, selects, and develops mitigations on risks associated with vendors and business partners. Inspected the annual risk assessments, based on the risk management template, to determine whether risks associated with vendors and business partners were evaluated based on identified threats and risk tolerances and to determine whether measures were specified to address the identified risks. Inspected the enterprise risk management system and General Data Protection Regulation (GDPR)- and IT Security surveys to determine whether mitigations on identified risks associated with vendors and business partners were documented and implemented in the risk register, risk assessment plans and risk assessments.	No deviations noted.
		CC9.2 - control B: Interxion's Management has, on a periodic basis, meetings with key vendors and business partners are held to discuss the identified risks and mitigating measures related to external stakeholders.	☒	☒	Inquired of management and inspected the Interxion Corporate Procurement Policy and Supplier policy to determine whether Interxion's requirements on regular meetings with key vendors and business partner were defined.	No deviations noted.

Ref.	Trust Services Criteria	Control specified by Interxion	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					For a sample of periodic meetings with key vendors and business partner, inspected the meeting invites, and/or meeting minutes to determine whether meetings were held to discuss the identified risks and mitigating measures related to the involved external stakeholders.	

5 Section V: Other information provided by Interxion Deutschland GmbH's Management

5.1 Digital Realty To Combine With Interxion

Management Statement

Interxion has entered into a definitive agreement to combine with Digital Realty, a global provider of data centre, colocation and interconnection solutions. This a unique opportunity to create a global platform and we expect this combination will enhance the products and services we offer our customers, as well as your ability to participate in communities of interest around the world.

Digital Realty will enhance Interxion's ability to serve multinational customers on a global scale whilst Interxion offers Digital Realty an opportunity to create a leading pan-European data centre footprint.

Digital Realty is a public company with operations around the world including North America, Europe, Asia, Latin America and Australia. By combining our highly complementary businesses, we will be in an even better position to serve our customers and create unique expansion opportunities for our customers across an even greater number of important and high-growth metro areas.

Specific benefits to customers include:

- Globally Expanding Connected Communities of Interest: The combined company will extend Interxion's successful strategy of creating and enabling valuable communities of interest in Europe by extending it across the combined company's global footprint. This combination will build upon Digital Realty's successful track record of hyperscale development and will represent an extension of the connected campus strategy that empowers enterprise customers to leverage the right products – from colocation to hyperscale footprints – to create value by efficiently deploying critical infrastructure and seamlessly connecting to a robust and growing universe of cloud platforms and connectivity service providers. The combined company will be uniquely positioned to meet the growing global demand from cloud platforms, service providers and enterprises seeking colocation, hybrid cloud and hyperscale data centre solutions as IT architectures are reengineered to support the explosive growth of data in modern business models.
- Complementary European footprint: Digital Realty's European footprint, including their established London and Dublin data centre portfolios, is highly complementary to our collection of 53 carrier- and cloud-neutral facilities in 11 European countries and 13 metro areas. These include our particularly strong presences in Frankfurt, Amsterdam, Paris and Marseille.

We look forward to our future together with Digital Realty, but for now, nothing changes. Until the transaction closes – which we expect to be some time next year – it remains business as usual, and both companies will continue to operate as separate entities. There should be no impact on your current service, and we will keep you updated on our closing process.

5.2 Interxion Deutschland GmbH Operational Excellence

Interxion Germany has been certified for the ISO 27001 standard for Information Security Management System and for the ISO 22301 standard for Business Continuity Management, for the ISO 9001 standard for the Quality Management System, for the ISO 14001 standard for the Environmental Management System, for the ISO 50001 standard for the Energy Management System, and for the PCI DSS standard for the Payment Card Industry Data Security System. In addition to these certifications,

Interxion Germany is involved in multiple programs and initiatives with a focus on energy efficiency and green IT.

5.3 Energy Efficiency

Interxion Germany joined the German Governmental Long-Term Agreements (LTA on Energy Efficiency (MJA) in 2008. The program involves a committed joint effort to work on energy efficiency measures with a controlled and documented process. Over a period of four years, energy saving measures are defined, evaluated, implemented, measured and reported annually. The consolidated results of the ICT segment are published by the Government every year. In addition, Interxion Germany purchases 100% green energy for its datacentres.

Interxion aligns its 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.

5.4 FRA 14: New Built, same Standards

During the reporting period of this SOC2 report Interxion Deutschland GmbH opened a new data centre, named FRA 14, with an equippable customer space of 4.980 m².

5.5 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.

5.6 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 Deutschland GmbH Operations team includes a specific Maintenance team. Interxion Deutschland GmbH implemented an advanced Maintenance Management System to manage, plan and document all maintenance activities, including an extensive asset database.

5.7 Management Response Regarding noted Findings

Interxion will initiate and define follow-up actions to remediate all findings identified during the SOC2 audit.