DIGITAL REALTY

Service Organisation Controls (SOC) 2 Report

Report on Interxion Deutschland GmbH's description of its cloud and carrier colocation data centre services on the suitability of the design and operating effectiveness of its controls relevant to security and availability throughout the period January 1, 2022, to December 31, 2022

May 23, 2023

Contents

1. Section I: Interxion Deutschland GmbH's Management Statement

We have prepared the accompanying "Interxion Deutschland GmbH's cloud and carrier colocation data centre services system for the period January 1, 2022 to December 31, 2022" (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) that may be useful when assessing the risks arising from interactions with the System throughout the period January 1, 2022 to December 31, 2022, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its principal 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 January 1, 2022 to December 31, 2022 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 January 1, 2022 to December 31, 2022.
c. The Service Organization's controls stated in the Description operated effectively throughout the period January 1, 2022 to December 31, 2022 to achieve the service commitments and system requirements based on the applicable trust services criteria.

As noted in Section IV of this report, the service auditor was unable to determine that controls related to the following Trust Services Criteria category: (common criteria related to) System Operations operated effectively during the period January 1, 2022 to December 31, 2022 to achieve the following Trust Services Criteria:

- 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.

Frankfurt, Germany, May 23, 2023

Interxion Deutschland GmbH

Volker Ludwig
Managing Director

Andreas Kederer
Director Operations

Ernst & Young Accountants LLP
Antonio Vivaldistraat 150
1083 HP Amsterdam, Netherlands
PO Box 7883
1008 AB Amsterdam, Netherlands

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

2. Section II: Assurance Report of the independent Service Auditor

To: management of Interxion Deutschland GmbH

Our qualified opinion

We have been engaged to report on Interxion Deutschland GmbH's accompanying "Interxion's cloud and carrier colocation data centre services system operated in Germany for the period January 1, 2022 to December 31, 2022" of its cloud and carrier colocation data centre services throughout the period January 1, 2022 to December 31, 2022 (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 January 1, 2022 to December 31, 2022 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 matters 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 January 1, 2022 to December 31, 2022 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 January 1, 2022 to December 31, 2022.

c. the controls stated in the Description 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 January 1, 2022 to December 31, 2022.

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

We were unable to determine that the following controls operated effectively to achieve the Trust Services Criteria 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.) throughout the period from January 1, 2022 to December 31, 2022. We refer to the description of tests of controls and results thereof in the Description of Tests and Results for more details:

- The control description for control CC7.1 - control A states that a formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities and that findings are remediated according to internal SLA's. We were unable to determine whether

follow-up for vulnerabilities and threats, which were identified in the vulnerability scans, was performed according to internal SLA's.

We performed our engagement 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 (Revised), 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information', issued by the International Auditing and Assurance Standards Board. 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 procedures

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

Our opinion is not modified in respect of this matter.

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 provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation 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 January 1, 2022 to December 31, 2022 and prospective user entities of cloud and

carrier colocation data centre services, 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" (Assertion) about 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) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description of the service organization's system; (5) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description; and (7) identifying the principal service commitments and system requirements and stating them in the Description.

Service auditor's responsibilities

Our responsibility is to plan and perform our procedures 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 procedures.

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 procedures 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 throughout the period January 1, 2022 to December 31, 2022. 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.

A reasonable assurance engagement 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 Description is 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 to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Amsterdam, May 23, 2023

Ernst & Young Accountants LLP

Dennis Houtekamer

Digitally signed by Dennis Houtekamer
DN: cn=Dennis Houtekamer, c=NL, o=Ernst & Young Accountants LLP
Date: 2023.05.23 08:12:40 +02'00'

drs. D. (Dennis) Houtekamer RE
Partner

Document reference: RITM5697660

3. Section III: Interxion Deutschland GmbH's cloud and carrier colocation data centre services system for the period January 1, 2022 to December 31, 2022

3.1. Introduction to DLR EMEA

3.1.1. DLR EMEA

Digital Realty (NYSE: DLR) and Interxion (NYSE: INXN) announced on October 29, 2019 that they have entered into a definitive agreement to combine their businesses to create a leading global provider of data centre, colocation, and interconnection solutions. As part of the integration, since September 2022 the Interxion branding is replaced by Digital Realty branding.

The combination of Digital Realty (hereafter DLR) and former Interxion (hereafter DLR EMEA) (hereafter combined as DLR Global), offers customers expansion opportunities across a greater number of important and high-growth markets - in fact, over 290 data centres across 47 metro areas, 24 countries and over 6 continents.

The integration and alignment of the Management Systems, resources, operational processes and tools is ongoing in 2022. The eventual result of the integration and alignment will be a country operations model for DLR EMEA (Europe Middle East & Africa) Operations, aligned with DLR's global Management System.

3.1.2. Background

DLR EMEA provides cloud and carrier neutral colocation data centre services in Europe from 61 data centres in 13 countries, across 15 cities (Amsterdam, London, Copenhagen, Stockholm, Frankfurt, Düsseldorf, Vienna, Paris, Marseille, Dublin, Brussels, Madrid, Zagreb, Athens and Zurich). The DLR EMEA head office is located in Hoofddorp, the Netherlands.

The data centres are strategically located to ensure they have power availability and connectivity. DLR EMEA 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. DLR EMEA 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.

In 2022 no changes have been made to the legal country entity names.

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's geographic accessibility allows comprehensive cable infrastructure access to worldwide telecommunications networks.

3.1.3. Service commitments

DLR EMEA 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.

DLR EMEA has defined the following principal service commitments:

- DLR EMEA is committed to maintain 99,999% uptime.
- DLR EMEA is committed to provide a vulnerability-controlled ICT system within logical and physically controlled environments.
- DLR EMEA is committed to meet agreed Service Level Agreements (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 separate 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 EMEA Command Centre (hereafter ECC) and the time of a service restoration by DLR EMEA.
    - **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.
- DLR EMEA is committed to maintain industry standard certifications and compliance programs in relevant entities, including ISO27001, ISO22301, PCI-DSS and SOC2 Type II (refer to 3.3.4 "Monitoring Activities").

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 DLR EMEA's 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 DLR EMEA 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)
DLR EMEA 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 3.3.10 Availability
DLR EMEA 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 and Physical Access Controls 3.3.7 System Operations 3.3.8 Change Management 3.3.9 Risk Mitigation 3.3.10 Availability
DLR EMEA 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 and Physical Access Controls 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
DLR EMEA is committed to maintain industry standard certifications and compliance programs in relevant entities, including ISO27001, ISO22301 and SOC2 Type II.	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 and Physical Access Controls 3.3.7 System Operations 3.3.8 Change Management

Key service commitments	Relevant section(s)
	3.3.9 Risk Mitigation 3.3.10 Availability

3.1.5. Organizational structure

The Global DLR Board of Directors consists of a Chief Executive Officer and six Board of Director members:

- President and Chief Financial Officer.
- Chief Human Resources Officer.
- Chief Revenue Officer.
- Executive Vice President General Counsel.
- Chief Investment Officer.
- Chief of Staff.

The Global DLR Board of Directors 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 and the Articles of Association. In all its dealings, the board shall be guided by the interests of the group as a whole, including the shareholders and other stakeholders. The board has the final responsibility for the management, direction and performance of the group.

The Chief Executive Officer (CEO) 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 management and the external reporting. The board's members are accountable to the shareholders at its Annual General Meeting of shareholders. Information Technology EMEA (hereafter IT EMEA) reports to the Chief Information Officer, who reports to the President and Chief Financial Officer.

Operations EMEA reports to the Group Managing Director, who reports to the President and Chief Financial Officer.

Human Resources EMEA (hereafter HR EMEA) reports to the Chief Human Resources Officer.

The EMEA Design, Engineering & Construction group hereafter (DE&C) reports to the Senior Vice President of Global Construction and Delivery, who the Chief Operating Officer. The Chief Operating Officer reports to the President and Chief Financial Officer.

The Organization charts on the next pages are a graphical representation of Global DLR, DLR EMEA and local DLR EMEA entities.

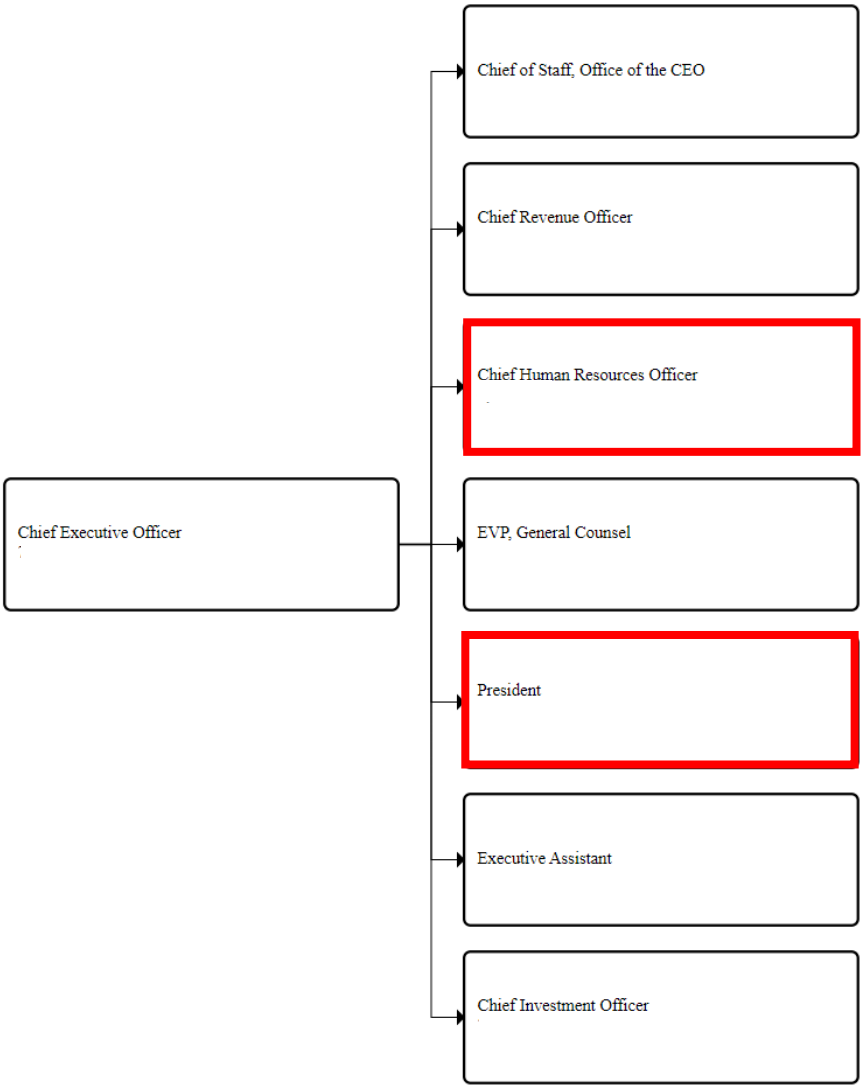


Figure 1: Chief Executive Officer and direct reports

Figure 2: Chief Financial Officer & President and direct reports

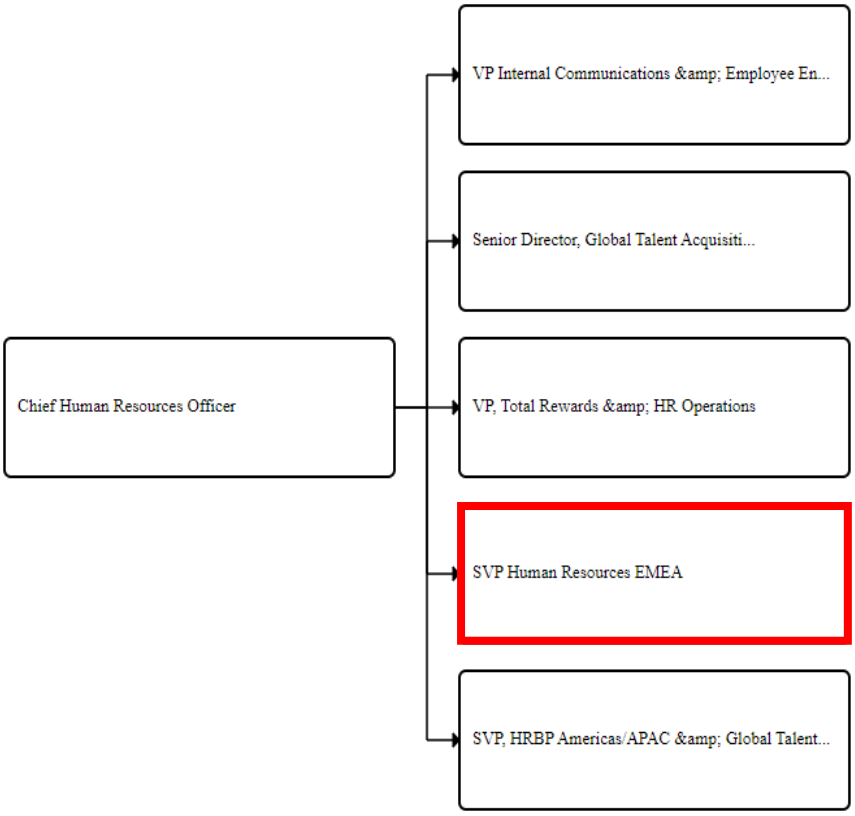


Figure 3: Chief Human Resources and direct reports

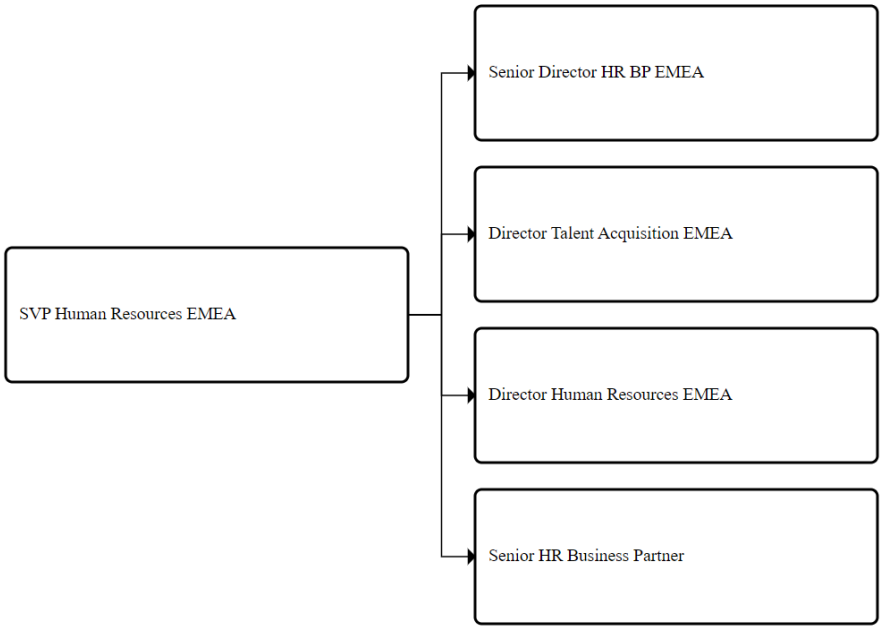


Figure 4: Senior Vice President Human Resources EMEA and direct reports

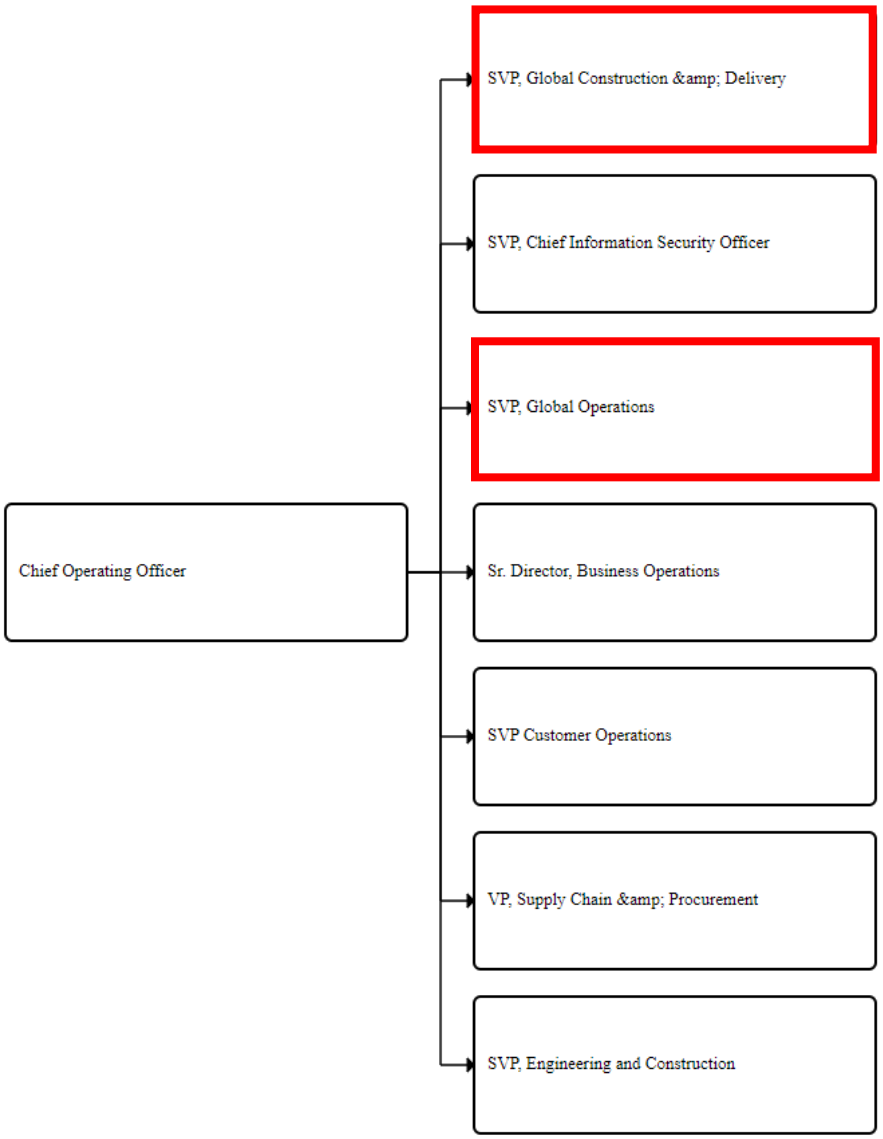


Figure 5: Chief Operating Officer and direct reports

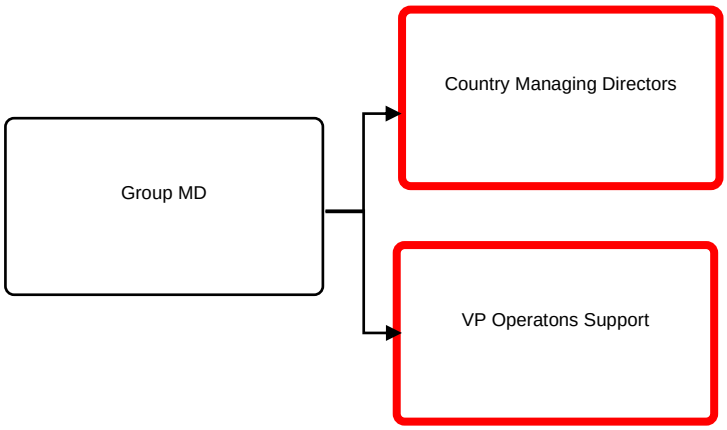


Figure 6: Group Managing Director and direct reports

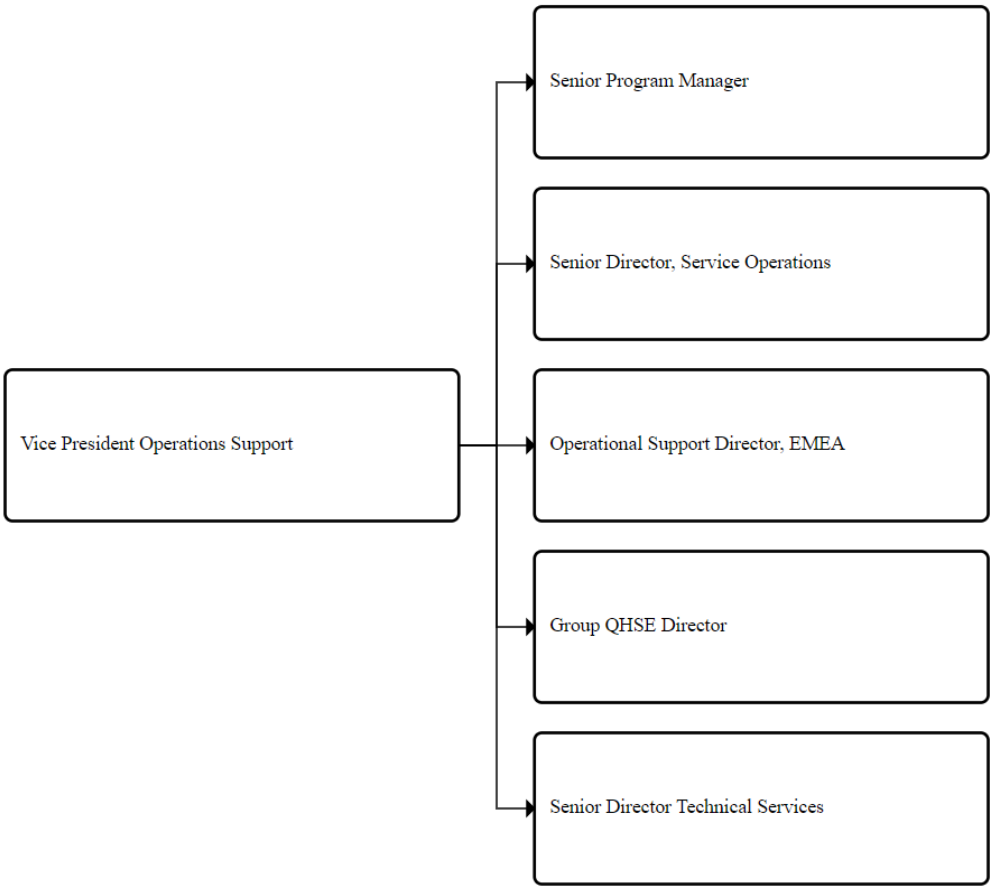


Figure 7: Vice President Operations Support and direct reports

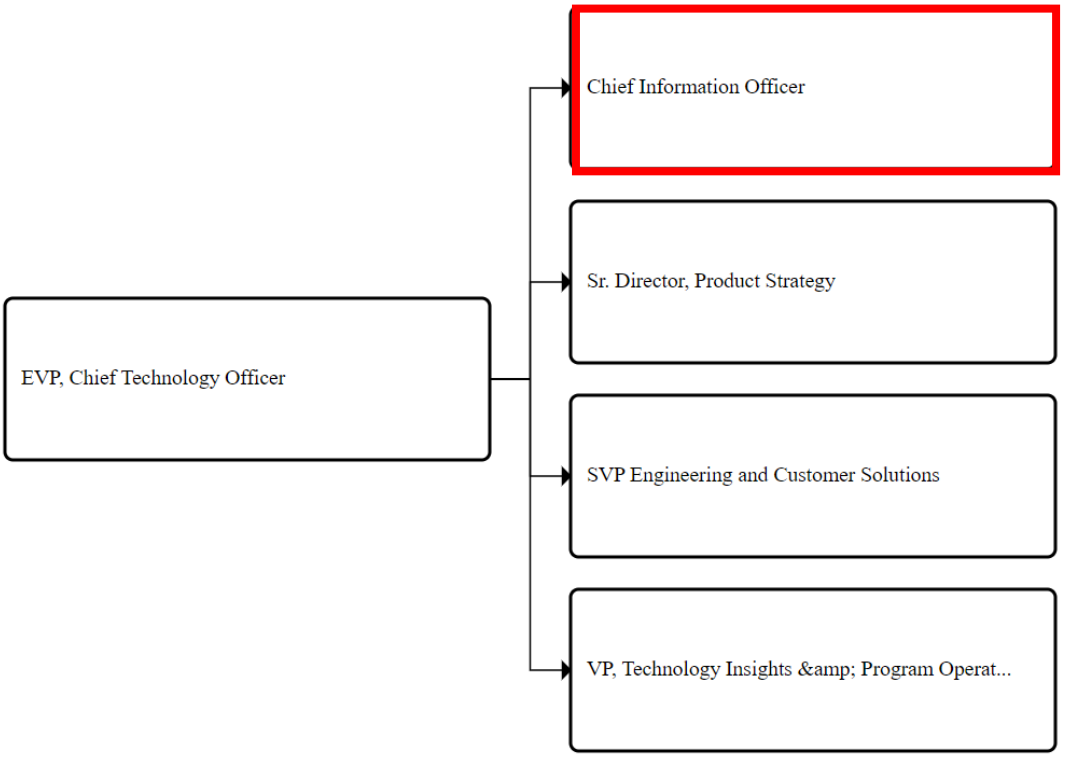


Figure 8: Executive Vice President Chief Technology Officer and direct reports

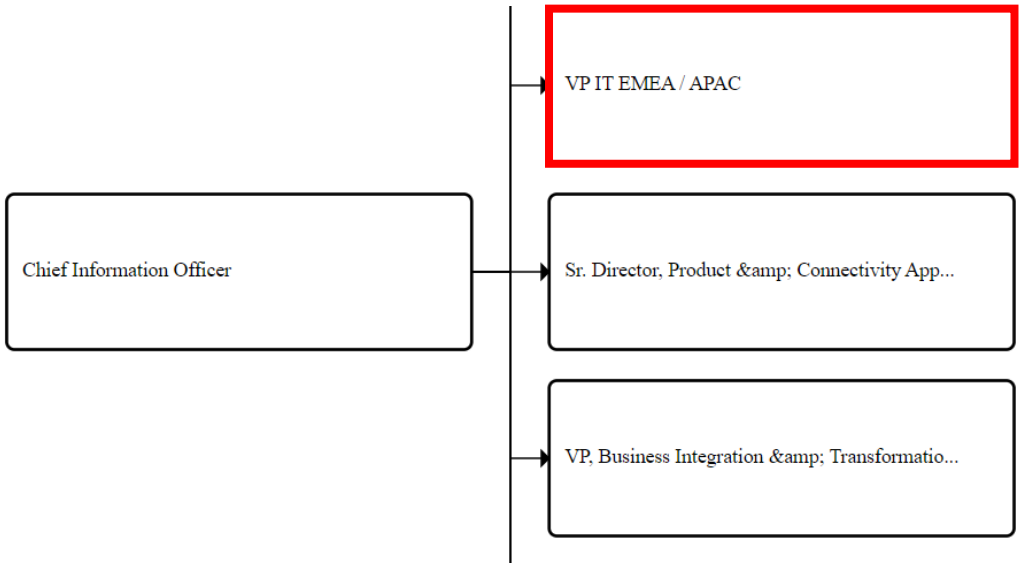


Figure 9: Chief Information Officer and direct reports

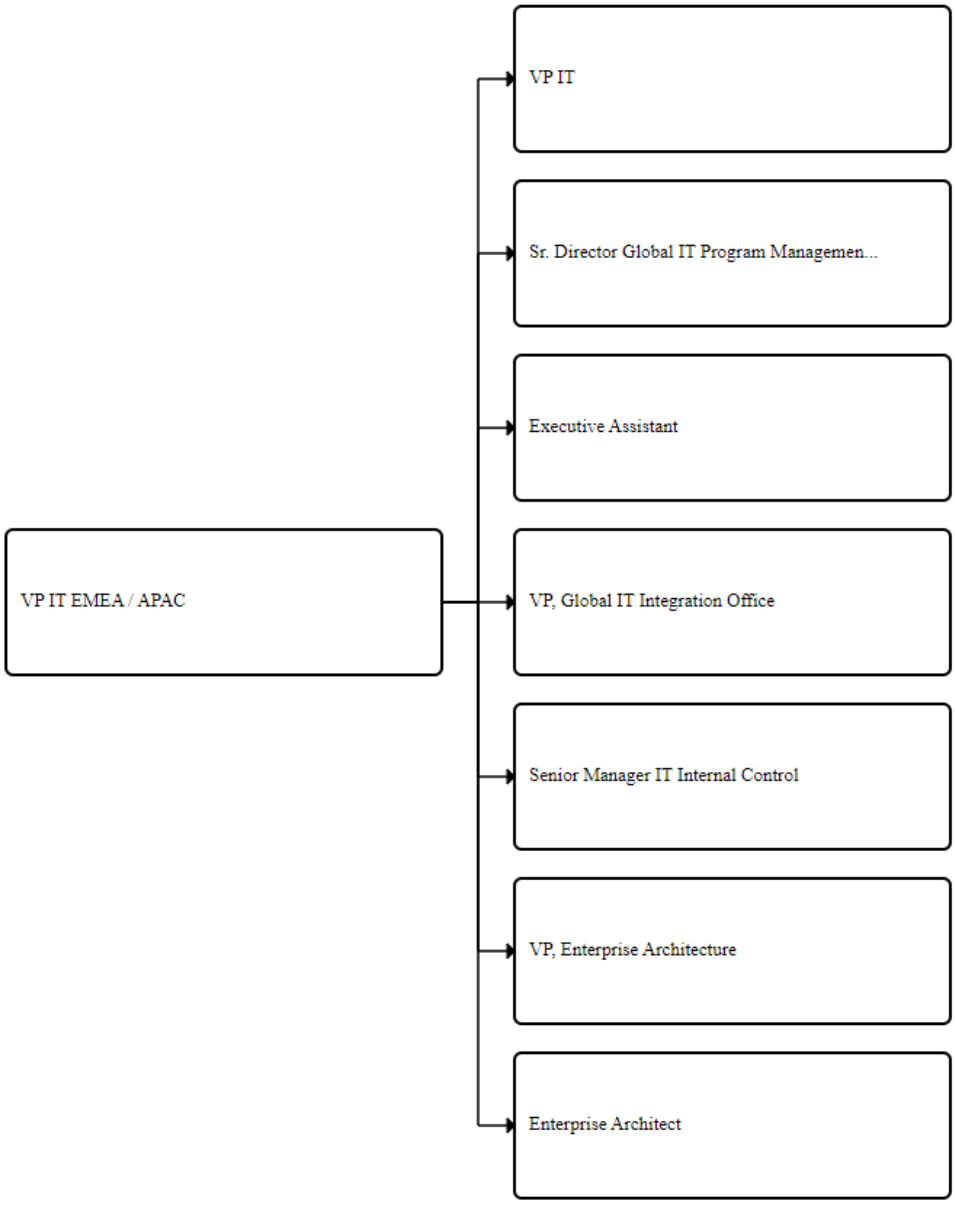


Figure 10: Vice President EMEA / APAC and direct reports

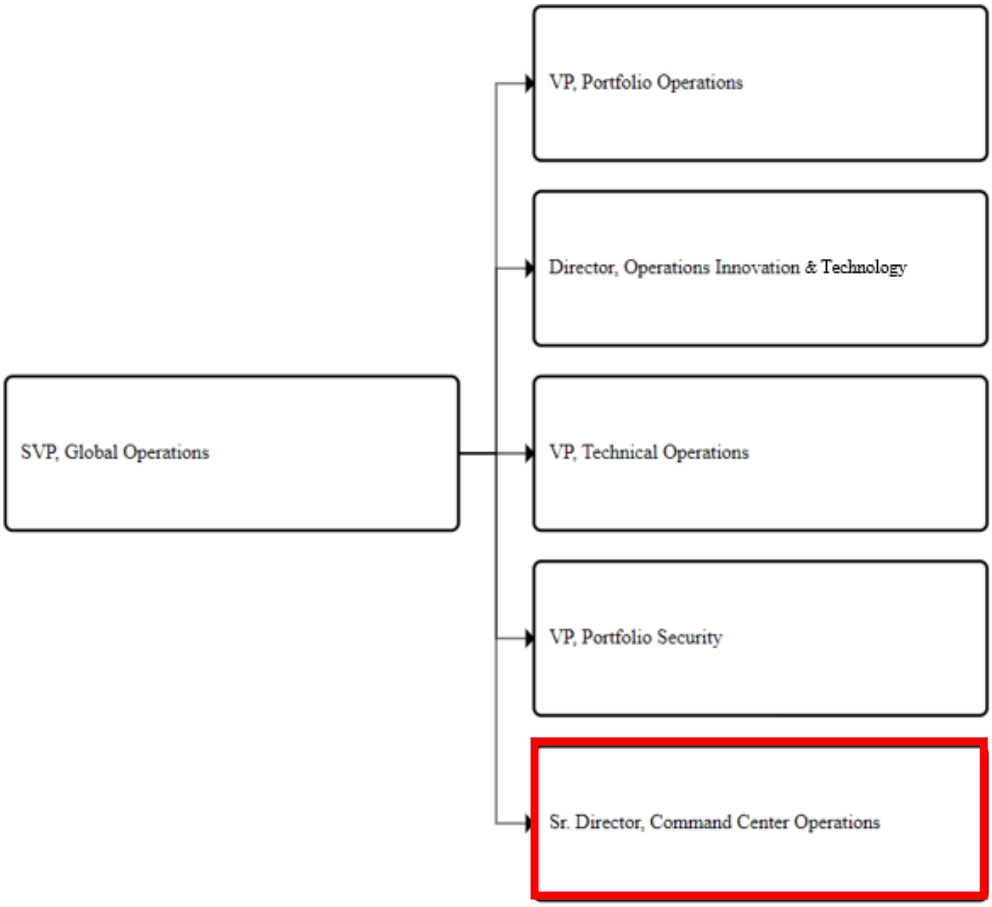


Figure 11: Senior Vice President Global Operations and direct reports

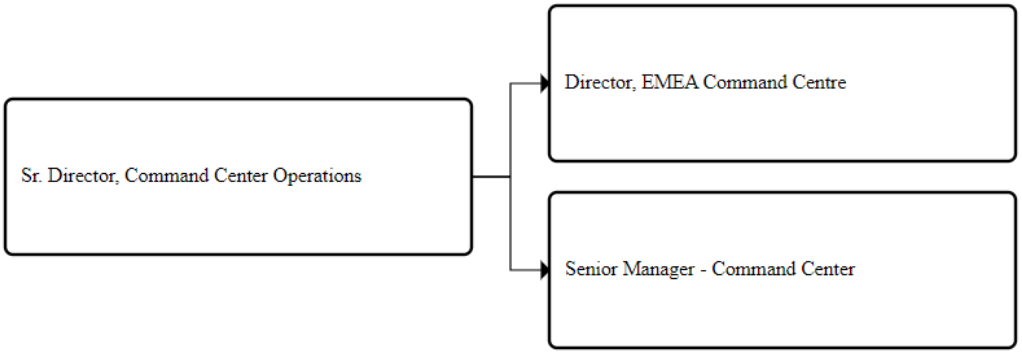


Figure 12: Senior Director, Command Center Operations and direct reports

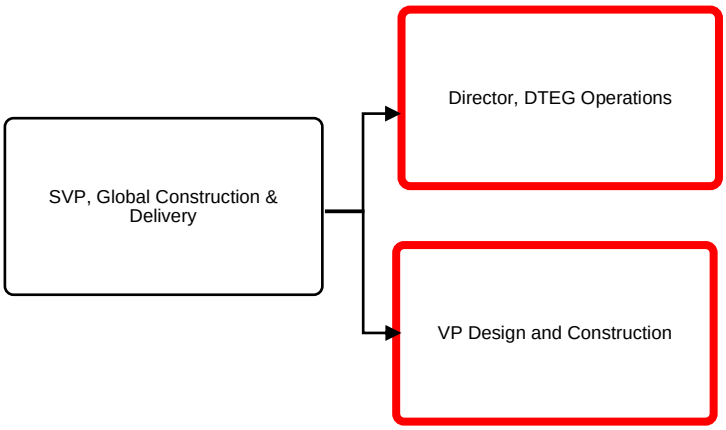


Figure 13: Senior Vice President Global Construction & Delivery and direct reports

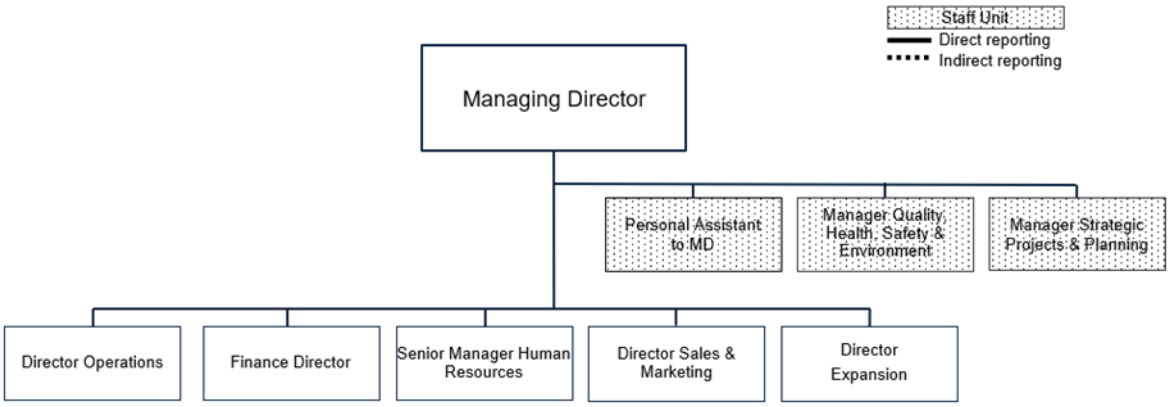


Figure 14: Organizational structure Interxion Deutschland GmbH, Managing Director and direct reports.

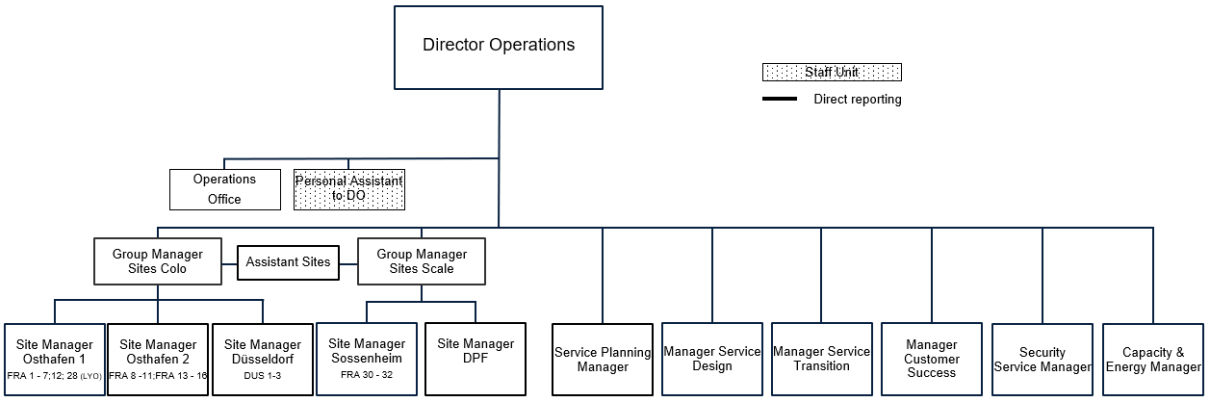


Figure 15: Organizational structure Interxion Deutschland GmbH, Director Operations and direct reports

Within DLR EMEA, the below mentioned departments operate together to provide a central hub and support for the local entities (Figure 7):

- Operations EMEA
    - Operations Support EMEA
        - QHSE EMEA (Quality, Physical Security, Health, Safety & Environment);
        - Platform Delivery EMEA (Customer Network Services, Cloud Service Provider Delivery, Service Excellence);
        - Technical Services EMEA (Asset Management, Maintenance Management, Change Management and Problem Management);
        - Operational Support EMEA (Reporting).
- EMEA Command Centre (ECC)
- Information Technology EMEA (IT EMEA)
- Human Resources EMEA (HR EMEA)
- Design, Engineering & Construction

The local entities are Interxion Netherlands, Denmark, Sweden, United Kingdom, Ireland, Switzerland, Austria, France, Belgium, Spain, Croatia, Greece and Germany. Each local entity has a dedicated local management team, responsible for data centre operations in their respective country. The Managing Directors within the local entity have a reporting line to the Group Managing Director. The local Operations Managers / Directors have a functional reporting line to the EMEA Vice President Operations Support. The local Quality and Security Managers report to the local organization and functionally to QHSE EMEA.

Interxion Deutschland GmbH has a dedicated team assigned to the operational management for Customers Services and Infrastructure Management. In the Interxion Deutschland GmbH headquarters, local teams support business and operations with Sales & Marketing, Finance incl. Procurement, Expansion, Quality and Human Resources departments.

Operations Support EMEA - QHSE EMEA

QHSE EMEA is responsible for the design, implementation and effective management of Governance, Risk and Compliance (hereafter GRC) within DLR EMEA and alignment with DLR Global. It supports the business, including local entities through a central compliance control framework, operating systems, communication and coordination and organizational structures.

QHSE EMEA is also responsible for the Governance of Physical Security and Health and Safety policies across the EMEA region.

Operations Support EMEA - Platform Delivery EMEA

Platform Delivery EMEA consists of the departments Customer Network Services, Cloud Service Provider Delivery and Service Excellence. Platform Delivery is responsible for the design, implementation and network configuration of customer solutions.

Operations Support EMEA - Technical Services EMEA

Technical Services EMEA is responsible for enabling the local entities to manage the data centre infrastructure adequately. Technical Services EMEA is responsible for Asset Management, Maintenance Management, Change Management and Problem Management.

Operations Support EMEA - Operational Support EMEA

Operational Support EMEA provides metrics that detail service performance to DLR EMEA customers, both internal and external. The Operational Support EMEA works closely together with local teams and relevant departments within the EMEA organisation and presents transparent, system agnostic data to qualify and measure performance to support a global view of operations, to allow continuous service improvement, scalability and ultimately improve the customer journey and experience.

EMEA Command Centre (ECC)

The ECC is the Single Point of Contact (hereafter SPOC) for DLR EMEA customers, part of the Global Command Centre that provides 24x7 support. The ECC team provides native language support in English, French, Spanish and German. In addition to being the SPOC for customers, the ECC provides remote monitoring on critical alarms linked to assets, as configured in the local Building Management System (BMS). The ECC acts as a gatekeeper for the local entities.

The ECC coordinates the preparation, approval and dispatch of customer notifications relating to critical events and planned maintenance activities. The ECC is working closely together with local teams and relevant departments within the EMEA organisation 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.

The ECC is also the knowledge hub for DLR EMEA data centres. It helps the DLR EMEA organization to optimise service and to track and improve customer focus.

Information Technology EMEA (IT EMEA)

IT EMEA is responsible for managing information technology related hardware and software assets supporting DLR EMEA’s colocation data centre services. Network management and firewall management (including access to the network) is provided by the DLR Global Network Engineering team.

Vulnerability management is executed by the DLR Global CRaaS (Cyber Resilience as a Service) team. Ownership of information technology lies within the DLR Global ITEO team.

ICT services are provided by the DLR Global ITEO team. For locally implemented server hardware and software assets by the local organisation, the DLR Global ITEO team supplies ICT services for access management to the network, backup, security, and other ICT related solutions where the ownership and responsibility remains with the local organization.

Human Resources EMEA (HR EMEA)

HR EMEA are managed locally and operated within a framework set by the Global Human Resource department that is then tailored where necessary to account for local legislation, custom and practice.

Wherever possible central management frameworks are provided for use by all countries within the DLR EMEA operation. These frameworks (such as remuneration, performance management and evaluation, benefits (private healthcare insurance and pensions), recruitment and background / security checking are all mandated and controlled by the Global 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.

DLR EMEA 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 a set of rules outlining the responsibilities and ethics and the statement of confidentiality and privacy practices', from this, employees are clear on what they are accountable for in their role, the integrity DLR EMEA expects them to exhibit and the ethics they should be demonstrating in all DLR EMEA business activity.

The AUP applies to every individual who uses Organizational information assets, and it sets out what the DLR Global considers to be the acceptable use of these assets. It outlines the DLR Global principles, which govern the use of the ICT network, and all ICT owned assets throughout the company. Each individual has to sign off for acceptance after reading the AUP.

There is a framework for functional training that is managed at DLR Global HR. Training is based upon the function an employee carries out. Besides the role-based trainings, the Global Data Privacy training and the Information Security Awareness training are mandatory for all employees.

Relevant qualifications are maintained and improved as appropriate. There are monthly cross-country HR meetings to ensure all countries are made aware of the agreed DLR Global HR policies and given an opportunity to state where central HR policies cannot be applied for the reasons given above.

Due to the nature of DLR EMEA's business, employee inductions are carried out at country level to address the responsibilities for security awareness within the data centre operations. This means that whilst acceptable use of DLR EMEA 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 in a global maintained HR Information System and managed locally.

Digital Technology Engineering Group (DTEG) / EMEA Design, Engineering & Construction (DE&C)

The Digital Technology Engineering Group (DTEG) has been restructured to EMEA Design, Engineering & Construction (DE&C) on July 21, 2022, and is managed by the VP EMEA DE&C. It consists of facility experts and establishes the current and long-term direction of data centre standards to help keep DLR EMEA data centres secure, highly reliable, competitive, green and energy efficient. DE&C provides the following services:

- Digital Technology (both Facility and IT Engineering).
- Engineering (both Facility and IT Engineering).
- Design Engineering Requirements (DER).
- Data Centres Construction Projects (new build, expansion etc.) - control, support and reporting.
- Digital / IT Engineering Projects - planning, management and implementation.
- Energy Saving programs - 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 DLR EMEA's Data Centres Audit Programs related to security, operational performance and technical level of country organisation including quality, compliance and Management & Organization matters.
- Governmental engagement with a pro-active approach to upcoming rules and regulations.

As a result of this restructure the position of Chief Engineering Officer ceased to exist, and the DE&C team is led by the Senior Vice President of Global Construction & Delivery.

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 Categories Availability and Security set forth in the American Institute of Certified Public Accountants (AICPA) section 100*, 2017 Trust Services 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, FRA13, FRA14, FRA15 and FRA16 (hereafter FRA01 to FRA16) and DUS01 & DUS02 locations in Germany. Data excluded from the scope of this report includes data, applications and hardware installed and managed by customers.

3.1.7. Responsibilities

The local DLR EMEA entities are responsible for compliance to local controls. QHSE EMEA is responsible for compliance to central controls and it supports the local DLR EMEA entities when information is managed centrally (e.g. Human Resource data). Core Central Company responsibilities are reflected through the scope of the report and pertain to the following departments: Operations Support EMEA, IT EMEA, HR EMEA and DE&C based in the United Kingdom and the Netherlands.

In addition, QHSE EMEA is coordinating the overall SOC2 program (maintaining the SOC2 framework, progress on compliance (internal and external testing)).

Refer to Section IV "Description of Criteria, controls, tests and results of tests" for the distinction between local and central DLR EMEA responsibilities and details of the Trust Services Criteria and related controls.

3.1.8. Subservice Organizations

In relation to the Trust Services Criteria and related controls as included in the Description no relevant subservice organizations have been engaged.

3.1.9. Changes to the Control Environment

Several changes have been made to the control framework. In 2022, the control framework was reviewed in-depth for further alignment with the DLR Global control framework as for some controls the ownership was transferred to DLR Global.

As of July 21, 2022, DTEG was restructured to EMEA Design, Engineering & Construction (DE&C) group, aligning it and reporting to DLR Global organization. This change has no impact on the control environment.

Until May 2022, the legacy software, Sage CRM was only used for external Customer notifications when attachments had to be shared. After May 2022 all functionality was migrated to ServiceNow.

for FRA8 and FRA9 smoke detection systems were installed in the generator containers since January 26, 2022.

On October 12, 2022 Jerrasoft (Biometric Control System) was shut down and the functionality was incorporated in PAC (Access Control System & Biometric Control System).

Below a summary of the changes to the control framework. To improve clarity for the organization, several other changes have been made to the control framework. These updates are considered minor changes with no impact on the controls; therefore, they are not listed below.

Control #	Control Description 2021	Control Description 2022	Details
This table only contains updates to the unique controls (and the updates to the corresponding referral controls are not repeated) except for any new referral controls.			
CC1.1 – control B	Hiring procedures include background checks or reference validation, which are performed by HR and retained electronically	Hiring procedures include background checks and reference validation, which are performed by HR and retained electronically.	Control wording was updated to align with the DLR EMEA hiring policy, requiring both background checks and reference validation.
CC1.2 – control A	CISO DLR is responsible for keeping the organisation aligned with Information Security and Service Organisation Standards as approved by relevant senior management or Board of Directors. CISO DLR ensures that inputs from all parts of the organisation are collected with respect to Information Security and addressed by senior management. Also, it communicates	The Board consists of Directors who qualify as independent under the NYSE listing standards. Such practices and performance against established requirements and expectations are publicly disclosed.	Based on the 2022 Risk Assessment procedures, the CC1.2 – control A (2021) control was removed from the control framework under Trust Service Criteria CC1.2, as the contribution of this control for achieving the Trust Service Criteria was limited compared to the newly introduced CC1.2 – control A (2022) control.

Control #	Control Description 2021	Control Description 2022	Details
	the expectations of senior management towards organisation in the areas of Information Security and Service Organisation. This happens through the DLR Global CRaaS platform which meets every month.		
CC1.2 – control B	Interxion has defined organizational structure, reporting lines, authorities, and responsibilities. These are revised when necessary to help meet changing commitments and requirements.	N / A	Based on the 2022 Risk Assessment procedures, this control was removed from the control framework under Trust Service Criteria CC1.2, as the contribution of this control for achieving the Trust Service Criteria was limited (compared to the other controls related to the Trust Service Criteria).
CC1.4 – control D	N / A	On an annual basis all employees are subject to a performance evaluation to review achievement of objectives and personal development plans.	New control introduced to further align with DLR Global control framework.
CC2.2 – control D	N / A	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. Refer to CC1.3 control A	Based on the 2022 Risk Assessment procedures, the control CC1.3 control A was considered additionally relevant for this Trust Service Criteria (CC2.2) and was added as referral control CC2.2 – control D.
CC5.1 – control A	Interxion's GRC Committee performs annual reviews and approves the Interxion Security and Availability policies and procedures. Interxion	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the	This control previously referred to the Governance, Risk & Compliance Council / Committee. The council ceased to exist in the course of 2021, and the

Control #	Control Description 2021	Control Description 2022	Details
	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.	associated system requirements. The policies and procedures are communicated to internal personnel via the GRC tooling. Refer to CC2.2 - control B	control description was not updated accordingly. Based on the 2022 Risk Assessment procedures, this control was removed from the control framework as a similar control was already described for CC2.2 – control B and could therefore be referred to.
CC6.6 – control A	External points of connectivity are protected by a firewall complex and an Intrusion Prevention System.	External points of connectivity are protected by a firewall complex and an Intrusion Prevention System. In case a firewall configuration needs to be changed or a new firewall needs to be created, it needs to be requested via ServiceNow and approved by the GlobalICT NetEng CAB and GlobalICT SecurityCompliance CAB.	Control wording was updated to better reflect the process, however the underlying process for DLR EMEA did not have substantive changes compared to 2021.
CC6.8 – control A	Anti-virus software is installed on workstations, laptops, and servers supporting such software. The software is updated on a (at least) monthly 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.	Anti-virus software agents are installed on workstations, laptops, and servers supporting such software. For updating the AI engines via releases, test groups are created before the releases are deployed. Devices that haven't been updated are reviewed periodically and follow up actions are taken.	Control wording was updated to further align with DLR Global control framework and processes.
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 and documented in an incident ticket. If vulnerability presents a significant risk a	A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal SLA's.	Vulnerability management is executed by the DLR Global CRaaS team. Ownership of information technology lies within the DLR Global ITEO team.

Control #	Control Description 2021	Control Description 2022	Details
	treatment plan is put in place to mitigate the vulnerability to an acceptable level.		
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.	N / A	Based on the 2022 Risk Assessment procedures, this control was removed from the control framework, as it was determined that the contribution of this control for achieving the Trust Service Criteria was limited (compared to the other controls related to the Trust Service Criteria).
CC7.1 – control D	Interxion performs a (local) management review on (at least) an annual basis on the local access groups which are enforced by the firewall rules (to limit access to the critical security and environmental systems). Follow-up actions resulting from the review are documented and monitored.	N / A	Based on the 2022 Risk Assessment procedures, this control was removed from the control framework, as it was determined that the contribution of this control for achieving the Trust Service Criteria was limited (compared to the other controls related to the Trust Service Criteria). Control CC6.6 – A was elaborated with firewall configuration aspects.
CC7.2 – control B	N / A	Any attempt of illegal access to the network is automatically monitored, detected and logged. Unauthorised devices are automatically diverted to an isolated VLAN. Configuration checks are performed on an annual basis to ensure the correct	Based on the 2022 Risk Assessment procedures, this control was added to the Trust Service Criteria, as it was determined that adding this control was enhancing the possibility for achieving the Trust Service Criteria and to substantiate the activities performed by the DLR Global ITEO and the DLR Global CRaaS team.

Control #	Control Description 2021	Control Description 2022	Details
		functioning of the application.	
CC7.3 – Control B	The resolution of security and availability breaches and incidents is reviewed at quarterly operations and security group meetings. Security breaches and incidents, with user or customer impact, are reviewed within the GRC Committee. Availability breaches and incidents, with user or customer impact, are reviewed in periodic OPS Support meetings and / or periodic MO meetings.	Security and availability breaches and incidents, with user or customer impact, are communicated to relevant stakeholders and when required reviewed in bi-weekly MO meetings	Control wording was updated to better reflect the process which is implemented by DLR EMEA, however the underlying process for DLR EMEA did not have substantive changes compared to 2021.
For the following controls the control wording was updated to further align with DLR Global control framework, however the underlying process for DLR EMEA did not have substantive changes compared to 2021: A1.1 – control B, A1.2 – control D, A1.3 – control A, CC1.3 – control A, CC1.4 – control A, CC1.4 – control B, CC2.1 – control A, CC2.2 – control A, CC2.2 – control B, CC3.1 – control A, CC3.1 – control B, CC3.2 – control A, CC3.3 – control A, CC4.1 – control D, CC6.1 – control A, CC6.3 – control A, CC7.1 – control B, CC8.1 – control A, CC8.1 – control B and CC8.1 – control D.			

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 central DLR EMEA responsibilities and details of the Trust Services Criteria and related controls.

3.2.1. Infrastructure

FRA01 to FRA16 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.

Based on the Design Engineering Requirement (containing the design requirements on the data centre setup) and in accordance with the risk assessment, environmental protections are in place to protect against environmental threats. These environmental protections receive Condition Based Maintenance, or Time-Based Maintenance. Condition Based Maintenance monitors the actual condition of the asset and shall be performed when certain indicators show signs of decreasing performance or upcoming failure. Time Based Maintenance is performed based upon predefined scheduled intervals.

The FRA01 to FRA16 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 threats. The facilities offer redundant (N+1) UPS power and redundant (N+1) cooling as well as alarm and monitoring systems. The FRA01 to FRA16 and DUS01 & DUS02 data centres support high-density power configurations and have been designed using an energy-efficient modular architecture, including free cooling and maximum efficiency components.

The following critical infrastructure systems (environmental protections) are in scope:

- Generators.
- Uninterrupted Power Supplies (UPS).
- CRAC's.
- Chillers.
- Fire detection systems.
- Fire suppression systems.
- Water leakage detection systems.

3.2.2. Software

DLR Global uses software (on Corporate, EMEA and local level) which are relevant for the security and the availability of their cloud and carrier colocation data centre services.

DLR EMEA uses Service Management software (Sage CRM / ServiceNow) and the (Customer) Portal to manage customer / service requests, including requests for access, deliveries, removals, 'Remote Hands and Eyes', customer enquiries, complaints, quote requests and event and incident management. Customers can also use the (Customer) Portal to update access rights for their rooms, cages and rack space.

Critical equipment alarm monitoring is performed through the local Building Management Systems (hereafter BMS). ECC receives critical alarms sent from the local BMS to a central database which is monitored by Alarm Monitoring tooling.

Ultimo is used to manage Change Requests and Configuration Management of critical data centre systems.

MetricStream is used as Governance, Risk and Compliance (GRC) software tool to manage internal compliance testing, document control, enterprise risks and audit management.

ServiceNow, (Customer) Portal, Sage CRM, Ultimo and MetricStream are maintained by DLR Global ITEO team and operated by Interxion Deutschland GmbH.

DLR EMEA uses several types of software (local level) to support their service provisioning. Whilst there is some regional variation the systems in scope 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
ServiceNow	Service Management Tool: registration of physical / logical access of the IT data centre infrastructure	DLR Global ITEO team
Ultimo	Maintenance Planning System	DLR Global ITEO team
Customer Portal	Front-end of the Service Now for receiving and managing customer requests.	DLR Global ITEO team
MetricStream	Governance, Risk and Compliance (GRC) tool	DLR Global ITEO team
Sage CRM	Platform to manage external Customer notifications (out of scope as of June 22nd, 2022.	DLR Global ITEO team
BVMS	CCTV monitoring	Interxion Deutschland GmbH FRA01 to FRA16
Pelco	CCTV monitoring	Interxion Deutschland GmbH DUS01 & DUS02
Jerrasoft	Biometric Control System	Interxion Deutschland GmbH FRA01 to FRA16 DUS01 & DUS02
PAC	Access Control System & Biometric Control System	Interxion Deutschland GmbH FRA01 to FRA16 DUS01 & DUS02
SOC	Security Incident management system	Interxion Deutschland GmbH FRA01 to FRA16 DUS01 & DUS02

Software	Functionality	Managed
EMS - Schneider Power Monitoring Expert	Power Monitoring System	Interxion Deutschland GmbH FRA01 to FRA16 DUS01 & DUS02
Schneider EcoStruxure Building Operations	Building Management System	Interxion Deutschland GmbH FRA01 to FRA16 DUS01 & DUS02

3.2.3. Governance, Risk & Compliance Board

In addition to the Operations Support EMEA department, DLR EMEA has established a Governance, Risk and Compliance Committee.

Within the GRC Committee the identified risks and risk treatment activities are discussed. The GRC Committee discusses and adopts changes affecting the Internal Control Framework. The GRC Committee makes decisions about raising employee awareness (including monitoring training progress). Results of internal and external audits, as well as significant Information Security incidents are reviewed within the GRC Committee.

The GRC Committee members are the Vice President IT EMEA, Senior Manager IT Internal Control (who also seats in the CISO meeting), Manager IT Internal Control, Senior Legal Counsel, QHSE Director EMEA, Senior Manager Compliance EMEA and the Senior Manager GRC.

3.2.4. Policies & Procedures

DLR EMEA employees adhere to the corporate policies and procedures that define how services should be delivered. These policies are available in the Document Management System in the DLR EMEA GRC (MetricStream) software tool.

3.2.5. Data

DLR EMEA performs an annual assessment of the required (quality) information / data 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.

Refer to 3.3.2 “Communication and Information” on the process within DLR EMEA on how internally and externally information / data is shared and reported.

3.3. Internal control environment

This section provides information about the interrelated components of internal control at DLR EMEA:

Control Environment

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

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

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

It demonstrates DLR EMEA's commitment to attract, develop and retain competent individuals in alignment with the objectives. DLR EMEA 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. DLR EMEA communicates compliance to internal control information with not only senior management but also appropriate employees and board of directors. DLR EMEA has internal controls around compliance communications with parties external to DLR EMEA 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. DLR EMEA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. DLR EMEA identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed. DLR Global considers the potential for fraud in assessing risks to the achievement of objectives. DLR EMEA 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. DLR EMEA selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of internal control are present and functioning. DLR EMEA 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. DLR EMEA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

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

DLR EMEA deploys control activities through policies, in which it is established what the expectations are. The procedures put policies into action and are organized as follows:

Logical and Physical Access Controls

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 DLR EMEA, System Operations are the processes and systems which manage, detect and mitigate processing non-conformities, including access (physical and logical) security non-conformities.

Change Management

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

Risk Mitigation

Risk Mitigation within DLR EMEA 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.

Availability

DLR EMEA 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. DLR EMEA 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. DLR EMEA tests recovery plan procedures supporting system recovery to meet its objectives.

3.3.1. Control environment

The objectives of the internal control structure are to:

- provide reasonable, but not absolute assurance as to the integrity and reliability of the organisation
- ensures the protection of assets from unauthorized use or disposition.

DLR EMEA has established and maintains an internal control structure that monitors compliance with established policies and procedures. The remainder of this subsection elaborates on the tone at the top as set by management, the integrity, ethical values and competence of DLR EMEA 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 DLR EMEA's assessment of risk facing the organization.

3.3.1.1. Integrity and ethical values

DLR EMEA is an industry-leading provider of carrier neutral internet data centre services. 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 DLR EMEA's industry, but also when it comes to acting in accordance with high ethical standards. It is a core value of DLR EMEA and one of the drivers for its future that it has and will remain true to its ethical principles, irrespective of how hard DLR EMEA competes and strives to improve the business.

DLR EMEA has a formal set of guidelines that explains the ethical principles that will be followed as it conducts business. This is contained within the Code of Conduct and sets out the principles that DLR EMEA, as a company, and as individuals will adhere to. The Code of Conduct also helps the employees to understand their responsibilities.

To that end, the Code of Conduct contains guidelines and information on how DLR EMEA should behave but also what DLR EMEA should do when unacceptable behaviour has been identified. Employees have a duty to report any known or suspected violations of the Code of Conduct, including any violation of any applicable laws, rules or regulations. Violations shall be reported immediately to the supervisor. The supervisor will contact the Legal department and / or the HR department, who will work with the employee and the supervisor to investigate the violation. DLR EMEA has also established

a whistle-blower service allowing employees to remain anonymous when reporting violations of the Code of Conduct.

3.3.1.2. Governance and Oversight

DLR EMEA has a comprehensive governance and oversight framework. DLR EMEA 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 / IEC (International Electrotechnical Commission) accreditation in Information Security and Business Continuity (legacy Interxion sites only). This is, by the nature of its business, essential. This is backed by oversight from board level.

The DLR Global Board of Directors meets as often as they deem necessary or appropriate or upon the request of any member of the board. The board has adopted rules, which contain additional requirements for the 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 among the DLR Global Board of Directors.

3.3.1.3. Personnel Security

Responsibilities for specific information security procedures are defined and documented in individual job descriptions. Staff have accepted their specific responsibilities as detailed in the AUP for which the individual is required to acknowledge acceptance before they are authorized to access organisational information assets. Specific responsibilities for third-party contractors (e.g. security guard) are transferred to the suppliers of these contractors.

Employee background checks are conducted for Security Guards and other employees based on the position of employment. Besides background checks, Employees are subject to a reference check upon hiring, to validate the CV of the candidate. 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 DLR EMEA unless specified in contracts.

3.3.2. Communication and Information

3.3.2.1. Internal Communication and Information

Operational Meetings are held with site personnel to update them on scheduled customer activities (i.e. new customers, installation in progress), infrastructure and facility activities (e.g. preventive \ corrective maintenance and major changes) and general information on people, organisation, trainings, projects and actions plans. The frequency of these Operational Meetings is determined by Interxion Deutschland GmbH’s management team.

In each department, periodic meetings are held to align strategy, analyse data, and act on common action plans, software deployment and improvements. Interxion Deutschland GmbH’s 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.

DLR Global 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.

Employees of DLR EMEA 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. Employees found to be in violation of security policies are subject to disciplinary action up to and including termination of employment. Employees are required to report security incidents and weaknesses.

3.3.2.2. External Communication and Information - Customers

Once a new contract is signed, the customer account is created in the Sales Management Software and Service Management Tool. At this stage also the Service Level Agreement, which includes DLR EMEA'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:

- ECC contact details.
- Raising issues.
- 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 a DLR EMEA facility, customers are asked to follow a set of "House & Safety Rules".

Customers can interact with DLR EMEA 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 DLR EMEA's 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 ECC.

In cases where an unforeseen event occurs such as an incident or the resulting need for an emergency change, the ECC manages the communication to the customer. The frequency of these communications depends on the severity of the incident.

Interxion Deutschland GmbH can provide reports to customers and hold regular meetings with customers as a contractual option. For some customers, DLR EMEA 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 local the operations teams, but all relevant data and information is shared via the aforementioned communications processes and mediums.

3.3.2.3. External Communication and Information - External stakeholders

DLR EMEA management has, on a periodic basis, meetings with key vendors and business partners to discuss the identified risks and mitigating measures related to external stakeholders.

The need and frequency of these periodic meetings is determined on the impact of key vendors and business partners on internal controls on security and availability of the data centre operations and documented in the (local) stakeholder overview.

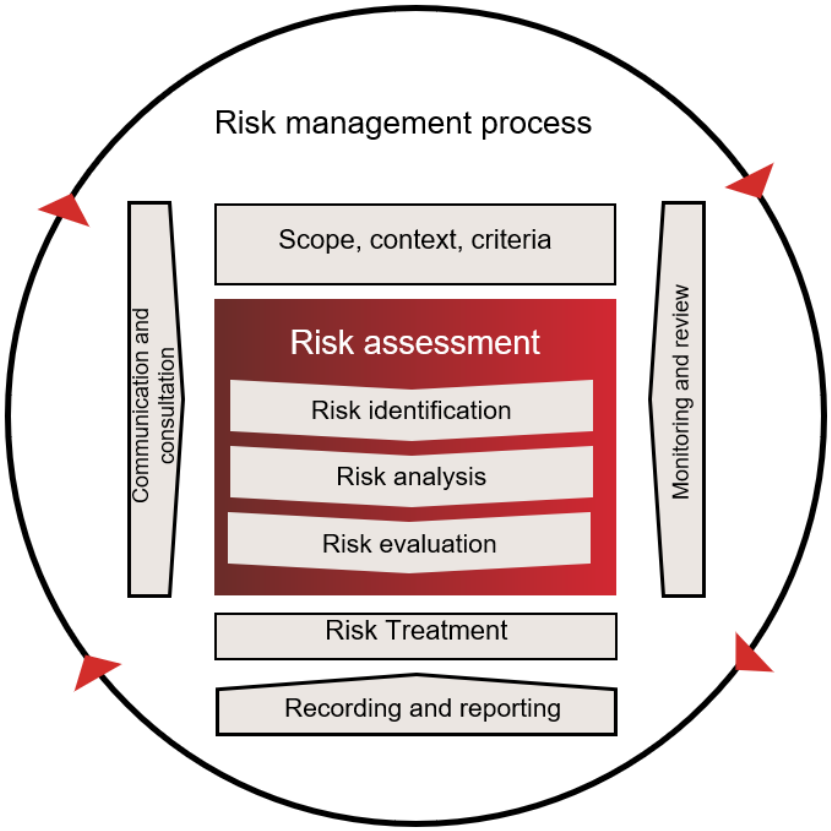
DLR EMEA informs relevant external stakeholders (contractors and suppliers) about the internal control environment by communicating DLR EMEA's requirements (House rules and Terms & Conditions for contractors and Non-Disclosure Agreements (NDA's) for Service Providers).

Key maintenance suppliers (for cooling, UPS, generators, security system and resources) 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. The need and frequency of these periodic meetings is determined on the impact of key vendors and business partners on internal controls on security and availability of the data centre operations and documented in the (local) stakeholder overview.

3.3.3. Risk Assessment

DLR EMEA follows the ISO 31000 standard to achieve effective risk management and realisation of business objectives. This risk assessment is based on business and control objectives that are aligned to the core values “Customer Focus”, “Teamwork” and “Result Driven”. DLR EMEA considers risk management as a core to creating, maintaining, and improving the control environment that results in quality, consistency and control effectiveness. DLR EMEA 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 DLR EMEA and country level to achieve both consistency and relevance through the organisation and capitalise on awareness and ownership.

Risks are assessed and evaluated according to the risk assessment process below:



DLR EMEA considers risk assessment as a continuous exercise and periodically reviews the assessed risks based on change in the external and internal contexts. QHSE EMEA is responsible for identifying and assessing changes that could significantly impact the system of internal controls as part of the risk management procedures.

DLR EMEA ensures that the risks to achieving the organisation's objectives are sufficiently mitigated. Risk treatment plans are recorded and assessed for effectiveness after implementation by the risk treatment plan owner.

MO meetings are held at monthly intervals 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.

The following changes are considered in the DLR EMEA’s 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. DLR EMEA 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. DLR EMEA continuously evaluates the risk of fraud within its business and has documented control processes that are independently attested.

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

DLR EMEA has clearly defined processes in place to monitor the services provided to customers and its internal controls. DLR EMEA buildings are supervised by on-site facility and security personnel, as well as the ECC 24x7. In terms of assessing the effectiveness of the controls, DLR EMEA 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 QHSE EMEA.

DLR EMEA 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. A review by QHSE EMEA is performed to determine 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 DLR EMEA'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. A Physical Site Security Audit is performed annually to verify the facilities, building, fence, security systems, CCTV, access etc.

At quarterly intervals a meeting is held with the data centre operation managers and the Vice President 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.

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

- Ensure compliance of policies and procedures with SOC2 / ISO27001 / ISO22301.
- Assessment of Information Security breaches initiate preventive actions where needed and relevant.
- Assessment of exceptions.
- Coordination of Risk Assessment and Risk Treatment Plans.
- Ensure adequate training / awareness related to Information Security and Business Continuity.
- Audit planning.
- Supplier Management follow up.

Network penetration testing is initiated by the Global Network Engineering team and is carried out by an approved external third party on an annual basis. The external party consists of senior security

consultants and engineers, who are experts in the field of enterprise system security. This test includes penetration testing on the external addresses that DLR EMEA 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 DLR EMEA brand and how it could be misused by a malicious attacker.
- Assessment of the infrastructure used to facilitate DLR EMEA'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.

A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal SLAs.

The primary focus is on access control. It evaluates the possibility of a hacker to:

- Gain access to confidential, classified, or secret information.
- Bring. substantial financial and / or reputational damage to DLR EMEA.
- Endanger the service continuity of the organization.
- Create a newsworthy incident.
- Endanger the safety of visitors, employees or customers.

Interxion Deutschland GmbH is continuously reviewing and improving the services provided to its customers (i.e. service quality, security of information, facilities). The following audits are performed at least once per audit cycle 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 9001 (Annually)
- External audit: ISO 9001 (per certification scheme)
- Internal audit: ISO 14001 (Annually)
- External audit: ISO 14001 (per certification scheme)
- Internal audit: ISO 50001 (Annually)
- External audit: ISO 50001 (per certification scheme)
- External audit: PCI-DSS (Annually)

3.3.5. Control activities

DLR EMEA Control Activities are supported by its 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 as "Tier 1" policies and procedures, mandated by the GRC Committee. The GRC Committee performs annual reviews and approves the DLR EMEA Security and Availability policies and procedures. DLR EMEA has published the policies and procedures via the GRC tool to employees. Local consultation is carried out within the group by the Quality and Security meetings, representing local Quality and Security Managers as well as Subject Matter Experts.

Management System policies and procedures are reviewed annually by QHSE EMEA. All other policies and procedures are reviewed by the process owner. QHSE EMEA monitors that all relevant policies and procedures are up to date. 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 the organization.

The Director QHSE EMEA has the mandate to approve EMEA Corporate policies and procedures related to the management system. For other processes the director of the relevant department has the mandate to approve policies and procedures. Where this is the case, it is noted within the document (e.g. for documents owned and managed by HR EMEA). These documents are reviewed at country level to ensure entities are fully aware of them and understand them.

The below is a list of all the categories available for document classification whether policies and / or procedures covered by this system description.

Document Categories	Type of procedural documents (Global / Regional (EMEA) / Local)
Business Continuity	Global: Business Continuity Policy and Procedure. Global: Business Continuity plans of IT infrastructure and processes. Local: Business Continuity plans of Data Centre operations.
HR	Global: HR Recruitment & Hiring Policy, Onboarding Policy. Training and Development Management, Performance Management. Local: Employee Handbook, local HR policies and procedures.
ICT	Global: Authentication policy, Encryption Policy, Acceptable Use Policy, Backup procedures, Vulnerability Management, IT Asset Management. Local: Local application access policies and procedures.
Legal	Global: Code of Conduct, Records Retention Policy.
Operations	Regional: Incident Management, Change Management, Maintenance Management, Asset Management, Emergency Operations, Event Management. Local: Emergency Operating Procedures, Alarm handling procedures.
Procurement	Global: Procurement Policy Local: Local Procurement procedures.
Quality	Regional: Management Review Procedure, Versioning and Classification, Information Security Policy. Risk Management procedure. Corrective and Preventive Action procedure. Local: Local IMS Policies, Audit Guidelines.
Security	Global: Physical Access Policy, Physical Security Standard. Local: Local Security Standard Operating Procedures.

3.3.5.1. Information Security Management

The senior management team has assigned lead responsibility for information security within EMEA to the EMEA Vice President 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).

DLR EMEA maintains an Information Security Management System (ISMS), 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 DLR EMEA 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 needs to comply with all relevant policies and procedures that DLR EMEA has in place to secure its systems services and business at all times. The resolution of security and availability breaches and incidents is reviewed frequently at operations and security group (GRC Committee and MO) meetings. Information Security breaches and incidents, with user or customer impact, are reviewed within the GRC Committee. Availability breaches and incidents, with user or customer impact, are reviewed in periodic Managing Operations (MO) meetings. In case of a high severity incident, periodic meetings are held between local Operations, Operations EMEA, ECC and relevant stakeholders, when applicable. These meetings due to the operational nature of the teams involved, are frequent though not always formal. Escalations and decisions are made in these meetings.

3.3.5.2. Monitoring and reporting

DLR EMEA selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of controls on security and availability are present and functioning. These evaluations are related to the system capacity, availability and security performance of the data centre operations.

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

The IT 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 DLR Global ITEO level to communicate current capacity and provide a framework for the business to inform IT 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 customer requirements.

Where contractually agreed, DLR EMEA 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);

DLR EMEA Group Reporting prepares KPI's on:

- 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. 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 DLR EMEA Vice President Operations Support.

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

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

Events impacting only local standard operational processes.

The responsibility for managing these events is with Interxion Deutschland GmbH's management and does not need external reporting. However, it will still be required for the Director Operations to ensure that involved personnel is 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. The local incident coordinator will inform the ECC in accordance with the Operational Incident Management Process.

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 the Vice President Operations Support EMEA and handled in accordance with disciplinary procedures and local laws and regulations. If required, the event shall be reported by the Director Operations to the customer contact.

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

The events should be reported by the Director Operations to the (Physical) Security Manager EMEA.

Events indicating existence of an external threat to DLR EMEA 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 EMEA Compliance Manager.

Interxion Deutschland GmbH's management team is required to ensure that personnel attending the premises is trained sufficiently to understand the rules and regulations and how to act on a physical / environmental incident.

Escalations of incidents are managed in ServiceNow. The Director Operations is required to retain a security event log documenting events and corrective actions and conclusions. Breaches and statistics are shared with the Director Operations. If a major incident is found (via the problem management process) to have an impact on other sites, these sites will be informed.

3.3.6. Logical and Physical Access Controls

3.3.6.1. Logical Access

There is a formal user registration and de-registration procedure for granting and revoking access to information systems and services. In the case of logical access to internal IT systems, requests for access are managed by logging a request in ServiceNow. The request is then approved by the line manager and the application owner.

Where appropriate and possible DLR EMEA ensures infrastructure components and software are required to be implemented with password submission and separate user ID and need to comply with the defined Global Password Management Policy for the Infrastructure components and software. 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 accounts are uniquely identifiable, while application generic accounts are in place if required. Two factor authentication is used for external access to the DLR EMEA network. For legacy applications that do not meet the requirements from the password management policy, mitigating measures are in place to reduce risks.

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 annually) 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 (by using a password management tool) which is only accessible for authorized personnel. Personnel with access to the generic accounts are included in an authorization list, 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 (non-AD) systems identified, appropriate controls are applied.

HR EMEA operates a policy of standard roles / functions. These roles are applied to each incoming employee based on which Active Directory (pre-defined) access groups (roles) are granted. This list of roles has inferred access limitations based on department needs and where applicable seniority. Formal role-based access controls to limited access to systems and infrastructure components are implemented on the DLR EMEA managed applications (Ultimo, ServiceNow and MetricStream) which use Active Directory (SSO) access groups. Due to application restrictions (e.g., no connection with network account possible) access granted to local systems and infrastructure components cannot always be implemented based on formal role-based access controls.

DLR EMEA maintains a tiered approach to its logical security. Where possible 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. DLR EMEA maintains a strict policy of Change Management on both its corporate and data centre environments. Any changes to the environment shall be approved by the Change Approval Board.

DLR EMEA maintains up-to-date firewall perimeters to maintain its central security. In case a firewall configuration needs to be changed or a new firewall needs to be created, it needs to be requested via ServiceNow and approved by the DLR Global ITEO Network Engineering CAB (GlobalICT NetEng CAB) and the DLR Global ITEO Security & Compliance CAB (GlobalICT SecurityCompliance CAB).

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.

DLR EMEA 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. All users of DLR EMEA systems must sign the Acceptable Use Policy. Users must adhere to the Information Security Policy.

IT ServiceNow 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.

It is company policy that anti-virus software agents are installed on workstations, laptops, and servers supporting such software. The AI engines are updated via releases which are tested before they are deployed. Devices that haven't been updated are reviewed periodically and follow up actions are taken.

3.3.6.2. Physical Security

DLR EMEA 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 is granted access. DLR EMEA 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 to FRA16 and DUS01 & DUS02 colocation data centres physical security controls are designed as a “building within a building” and include:

- The data centres FRA01 to FRA16 and DUS01 & DUS02 are permanently secured by security guards that are present 24x7 on site.
- The data centre perimeters are protected by surveillance cameras / Closed-Circuit Television (CCTV), alarm system (sound and visual) and infrared sensors, covering the whole perimeter (in and around building), which are monitored 24x7 by Security.
- Access control system that monitors and registers any entries or exits in the building, private rooms and other private spaces.
- Equipment to prevent unauthorized access to customer equipment:
    - Proximity cards, typically combined with biometric readers
    - Mantraps
    - Burglar alarm systems
    - Fence (FRA01 to FRA16)

DLR EMEA provides additional levels of security upon customer request to cages and cabinets (i.e., badge system, biometric readers at an entrance, video camera, etc.).

Procedures are in place for granting temporary and permanent physical access rights to the data centre for visiting contractors and 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.
- the sharing of access badges and tailgating are prohibited by policy.

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 the ECC. Access requests are processed according to Customer Change List Authorizer credentials and parameters and assigned to

Security at the specific data centre. Access revocations shall be processed within 30 days. In case access revocation requests must be processed immediately, the customer shall ensure that DLR EMEA is contacted by phone.

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 showing a government issued ID 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 DLR EMEA personnel. Badges must be worn clearly visible, and visitors must identify themselves to security personnel when requested to do so.

DLR EMEA employees and contractors' physical access to the data centres, technical rooms, offices, etc. is limited to specific levels of authorisation. The Managing Director is responsible for authorizing access to these areas. Security levels and access rights are reviewed on a periodic basis. Permanent and temporary physical access rights are managed through the Customer Portal.

3.3.7. System Operations

3.3.7.1. Vulnerability management

A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities through weekly scans. In addition, DLR EMEA performs an annual scan on the configuration settings of critical applications. In case vulnerabilities are detected corrective actions are initiated and followed-up. Vulnerability scans are reviewed as part of the yearly schedule of audits. Vulnerabilities are consistently assessed with regularity as prescribed in the Vulnerability Management procedure.

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). High value or high-risk systems are treated ahead of other systems.

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.

The allocated asset manager of each operational system is responsible for:

- monitoring vulnerabilities and vendors' releases of patches and fixes.
- installing operational software updates, patches, and fixes on the operational systems.
- maintaining the test environment, testing operational software updates and new implementations.

The DLR Global VP ITEO is responsible for the live operational environment.

The allocated asset manager of each operational system is responsible for defining and reviewing the security baseline of the critical systems. These documented baselines are used as templates to configure the critical systems accordingly. DLR Global CRaaS performs an annual scan on these systems. The configurations of the systems are compared against the baseline settings. In case unauthorized changes to the configuration on the critical systems are detected, corrective actions are initiated and followed-up.

3.3.7.2. 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 the ECC. The ECC will follow-up on alarm notifications with the local entity (engineer) whether further escalation is necessary.

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

Any attempt of illegal access to the network is automatically monitored, detected and logged. Unauthorised devices are automatically diverted to an isolated VLAN. On a daily basis the functioning of the configuration is monitored. In case the configuration needs to be changed it will be handled via the configuration management process.

3.3.7.3. Incident Management

In case of an incident, an incident coordinator both on-site and at the ECC is appointed, communicating on the progress to resolution so that the ECC can inform customers accordingly.

During an outage, communication may also be established via a conference bridge key people on site, usually the Director Operations, the Site Manager, Operations Support EMEA and a DC&E 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 ECC. The ECC 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 Operations Support EMEA.

The Operational Incident Management procedure categorizes the Incident on DLR EMEA 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 Operational Incident Management procedure aims at managing resources and the communication of incidents impacting customers.

Security and availability breaches and incidents, with user or customer impact, are reviewed in periodic Managing Operations (MO) meetings. The Managing Operations (MO) meetings are bi-weekly calls between the Directors / Managers Operations, Vice President Operations Support EMEA and the Director ECC, to align activities and administrative aspects, including major events.

3.3.8. Change Management

Changes to the data centre that impact the customer, infrastructure or monitoring systems are approved by Senior Management prior to installation in accordance with the DLR EMEA change management procedure. Changes may be implemented during ongoing service delivery to 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.

Changes to the data centre that may impact the customer, infrastructure or monitoring systems are reviewed by the Change Approval Board (CAB) prior to approval. The goal of the CAB is to provide cross-functional visibility for all data centre change requests, to assist the Change Management team in the impact level assessment as well as approve or deny change requests. The members of the CAB are dynamically assigned, based on the parameters of the Change Request. For data centre change requests (changes to the DC that impact customer, infrastructure and monitoring systems), involved roles can be:

- Senior Director of Technical Services.
- Director ECC.
- Director Operations or Managing Director.
- DC&E.
- Change Coordinator / Administrator.
- Technical Reviewer.

This is to ensure that the change has 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 customers 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.

Incidents which are classified by DLR EMEA as 'high severity incidents' are managed via the Incident Management Procedure and logged and followed up in ServiceNow. A Change Request or an Ultimo work order ticket is created to document further follow up / corrective actions, when required. ‘High Severity’ incidents can have emergency changes raised against them applying the risk assessment approach and respecting greater urgency. Customers are notified of changes that have potential customer impact. The high-level steps for change management are:

- Step 1: Initiate change request.
- Step 2: Review and approve change request through the Change Approval 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 DLR EMEA before changes are implemented.

3.3.9. Risk Mitigation

DLR EMEA 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 is offset with insurance policies that would otherwise impair the company objectives to be realised.

Regarding the process around risk mitigation regarding vendors and business partners refer to 3.3.2.3 “External Communication and Information - External stakeholders”.

3.3.10. Availability

3.3.10.1. Capacity

DLR uses software to measure system utilization on systems where this is critical. Alerts are generated when specific predefined thresholds are met. In case thresholds are met, follow up actions are initiated the by DLR Global ITEO.

From a data centre operations perspective, capacity requirements are evaluated by the Interxion Deutschland GmbH's Operations team on signing of initial contract and ongoing to contract renewal. The input from this Capacity Review is provided by the Sales departments. After the Capacity Review, Sales is informed about the available capacity. Documentation is managed locally and not within a single system.

3.3.10.2. Environmental systems

Power Supply

DLR EMEA 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 signage and emergency contact information is at hand. 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, DLR EMEA operates Very Early Smoke Detection Apparatus (VESDA) systems. In case of smoke, this system immediately alerts staff allowing them to take appropriate action before a fire starts.

Water Leakage Detection

DLR EMEA facilities include leak detection systems installed in areas that may be susceptible to leakage. The leak detection immediately alerts staff allowing them to take appropriate actions.

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.

DLR EMEA facilities are supervised by on-site security personnel, as well as the ECC 24x7. Moreover, critical alarms raised on the Building Management System (BMS) are monitored 24x7 in the data centre at the security office by the security guard, at the ECC and by the on-call engineers.

3.3.10.3. Preventive maintenance

DLR EMEA has defined a Maintenance Policy for the environmental protections in the data centre and contains a specification of the assets and their criticality, which are subject to planned maintenance.

In principle environmental protections receive maintenance on at least an annual basis, however for assets which are subject to condition-based maintenance other maintenance frequencies may apply in accordance with the Group Maintenance Policy, manufacturer's specifications or supplier requirements as well as local regulations e.g. electrical requirements.

DLR EMEA 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.

3.3.10.4. Data backups

Full weekly backups and incremental daily back-ups are taken of system critical data. The organization's information assets are subject to backup requirements, excluding mobile devices, and corporate workstations. 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 DLR Global VP ITEO 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 DLR Global VP ITEO 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.
- Backups are monitored daily and restores are tested at least annually.

Changes to the back-up schedule are approved by the DLR Global VP ITEO.

3.3.10.5. Business Continuity

DLR EMEA 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 DLR EMEA 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 DLR EMEA 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.

3.4. Trust Services Criteria and Controls

The Trust Services Criteria and the related controls to meet these Trust Services Criteria are specified by DLR EMEA and are listed in the accompanying Section IV: "Description of Criteria, controls, tests and results of tests". The Trust Services Criteria and related controls are an integral part of the Description.

3.5. Key User Responsibilities

DLR EMEA has designed and implemented its controls to meet its commitments and requirements as it relates to the Trust Services Categories security and availability. DLR EMEA 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 colocation data centre services 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 responsibilities of customers.

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

CC6.5: 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.

Customer management is responsible for:

- Ensuring that only authorized customer personnel have access to the customer equipment and space of the customer.
- Ensuring that access to customer equipment and space is restricted to authorized personnel via Access Control Lists (ACL) maintained by the Customer Change List Authorizer and administered by the ECC. These are procedurally integrated with each data centre Badge Management System. It is the responsibility of the customer to maintain an accurate ACL for its equipment.
- Ensuring that the Access Control List is reviewed periodically.
- Ensuring that access requests to FRA01 to FRA16 and DUS01 & DUS02 are submitted via the Customer Portal in advance by authorized requestors only.
- Ensuring that changes to authorized requestors and approvers are performed on the Customer Portal, however the preferred method is for customers 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 FRA01 to FRA16 and DUS01 & DUS02 reception desk.
- Ensuring that equipment is secured as necessary, including locking cages and racks. Physical security beyond the final access to the specific customer rack is the sole responsibility of the customer.
- Ensuring that DLR EMEA is contacted by phone in case access revocation requests must be processed immediately.

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.

Customer management is responsible for:

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

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.

Customer management is responsible for:

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

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 DLR EMEA, EY considered the aspects of DLR EMEA's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

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

4.2. Testing of Information Produced by the Entity

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

4.3. Trust Services Criteria and Controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified. They are the responsibility of DLR EMEA. The testing performed and the results of tests are the responsibility of EY. 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 Communication 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 Controls (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 Service Criteria	Control specified by DLR	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**: The local Operations team reviews DLR's system capacity, availability and security performance on a monthly basis. Corrections and other necessary actions are taken when issues are identified. Refer to CC4.1 - control A	X		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 for the issues identified by DLR's local Operations team.	No deviations noted.
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 B**: For business critical IT infrastructure, organisation shall establish mechanisms to monitor and rectify capacity issues.		X	For a sample of servers for in-scope systems and infrastructure components, inspected the supporting documentation to determine whether the system was being monitored for service availability and capacity (system utilization) and that breaches of predefined thresholds were identified by generated alerts to rectify capacity issues.	No deviations noted.
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 C**: Capacity requirements are evaluated by the local Operations team on signing of initial contract and ongoing to contract renewal. Documentation is managed locally and not within a single system.	X		Inspected power usage reports, monthly floor space reports and meeting documentation to determine whether the capacity requirements on power usage and available floor space was regularly evaluated by the DLR's local Operations team. For a sample of new DLR EMEA customers and contract renewals during the examination period, inspected the DLR's local Capacity	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					Manager's approval on capacity and space in the customer registration tool to determine whether the capacity requirements were evaluated upon signing of the (initial / renewed) contract and documented in locally managed capacity evaluation documentation.	
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**: DLR ensures that all new data centre and build outs (extensions) are commissioned as per the Design Engineering Requirements (DER) which is reviewed on at least an annual basis and must be approved by the CEO (Chief Engineering Officer) before release. Based on the Design Engineering Requirement and in accordance with the risk assessment, the data centre is protected by environmental protections: Power supply: - 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. Fire prevention and suppression: - Smoke detection systems (including standard and / or VESDA) - Automatic gas-based fire suppression systems - Hand-held fire extinguishing systems - Compliance with local regulatory requirements Water leakage detection and prevention: - Water leakage detection systems	X		Observed the data centre and inspected supporting documentation to determine whether multiple power feeds were available and whether UPS and generator systems were installed, in accordance with the Design Engineering Requirement and the risk assessment. Observed the data centre and inspected monitoring tooling and alarm documentation to determine whether smoke detection (standard and / or VESDA) and fire suppression systems (gas-based, water-based or 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. Observed the data centre and inspected supporting documentation to determine whether floors were elevated (raised floors), if required, and water leakage detection systems were installed to protect the data centre against water damage, in accordance with the Design Engineering Requirement and risk assessment.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		- raised floors (if required by the risk assessment) Cooling infrastructure: - Redundant CRACs and chiller units. - Temperature and humidity monitoring system.			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.	
				X	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 approved by the CEO (Chief Engineering Officer) before release.	No deviations noted.
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**: DLR has defined a Group Maintenance Policy for the environmental protections in the data centre and contains a specification of the assets and their criticality, which are subject to planned maintenance. In principle environmental protections receive maintenance on at least an annual basis, however for assets which are subject to condition-based maintenance other maintenance frequencies may apply in accordance with the Group Maintenance Policy and supplier requirements.	X		Inspected the Group Maintenance Policy document to determine whether environmental protections in the data centre have been defined and whether it includes a specification of the assets and their criticality, which are subject to planned maintenance. For a sample of environmental protection systems, inspected the maintenance report to determine whether maintenance has been performed on at least an annual basis (or according to the frequency as defined in the Group Maintenance Policy).	No deviations noted. For one (1) out of twenty-five (25) randomly selected environmental protection systems we determined that the scheduled maintenance has been postponed due to an incident and per request of a customer. In addition, back-up components of the environmental protection system were required to be replaced before maintenance could be performed, as maintaining the system without the required back-up component replacements would increase the risk of service disruptions during maintenance. The overall risk for postponing the maintenance was also (retrospectively) documented as low, in a risk assessment performed and approved by the Interxion Deutschland GmbH Site Manager.

Ref	Trust Service Criteria	Control specified by DLR	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 C**: Every data centre facility has 24 / 365 alarm monitoring (Building / DC Monitoring Systems - BMS / DCMS) in place for environmental threats (power supply failures, fire, water leakage hazards, temperature and humidity monitoring) and is monitored by the local Operations team. In addition to the local monitoring, ECC logs and monitors 24 / 7 environmental alarms received on the Group Critical Alarm Platform (GCAP) for all DLR entities to ensure timely response and communication with customers and stakeholders.	X		Inquired of management, observed the data centre and inspected monitoring tooling and alarm documentation to determine whether 24 / 365 monitoring on power supply related, fire related, water leakage, temperature and humidity alarms by the DLR's local Operations team, was performed.	No deviations noted.
				X	Inquired of management and inspected the GCAP monitoring system and mapping of environmental protection assets for the in-scope data centres in the GCAP monitoring system to determine whether 24 / 365 monitoring on power supply related, fire related, water leakage, temperature and humidity alarms, by the ECC, was possible for the mapped assets to ensure timely response and communication with customers and stakeholders.	No deviations noted.
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**: For all business-critical IT infrastructure, organisation shall take full and incremental back-ups according to approved back-up procedure. The back-ups shall be monitored and after 5 continuous back-up failures in one set there shall be an investigation and remediation performed and documented.		X	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 servers for in-scope systems and infrastructure components, 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 servers for in-scope systems and infrastructure components and days, inspected the	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					backup job completion report, to determine if backup was successfully completed. Per inspection of ServiceNow we determined whether backup completion was monitored on a daily basis by DLR Global ITEO employees and determined that in case of faults, failures or errors of backups incident tickets are created and in case of 5 continuous back-up failures in one set an investigation and remediation was performed and documented.	
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**A1.3 - control A**: Disaster recovery personnel perform an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements.	X		Inspected disaster recovery plan procedures to determine whether the availability commitments and system requirements for the critical environmental protections systems in the data centre were documented. Inspected the annual disaster recovery test reports, of the critical environmental protections systems in the data centre, to determine whether DLR's local disaster recovery personnel has tested the disaster recovery procedures based on a documented scheduled plan and on an at least annual basis.	No deviations noted.
				X	Inspected disaster recovery 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 and replication tests has been tested by the Global ITOE team on an at	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					least annual basis. Inspected the annual disaster recovery test report, of the critical environmental protections systems in the data centre, to determine whether DLR EMEA's disaster recovery personnel has tested the disaster recovery procedures based on a documented scheduled plan and on at least annual basis.	

4.5. Criteria related to the Control Environment

Ref	Trust Service Criteria	Control specified by DLR	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 (at least) annually thereafter.	X	X	Inspected the Code of Business Conduct and Ethics, the Acceptable Use Policy, the FCPA and Anti-Corruption Compliance Policy and Insider trading 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 DLR EMEA employees who were hired or transferred during the examination period, inspected the Mandatory Policy Attestation overview to determine whether new hires read the Code of Business Conduct and Ethics, the Acceptable Use Policy, the FCPA and Anti-Corruption Compliance Policy and Insider trading policy and accepted and formally affirmed these responsibilities upon hire by signing the Confirmation of Receipt (CoR) timely upon hire in accordance with the Local Recruitment Process Guide. For a sample of DLR EMEA employees, inspected the Mandatory Policy Attestation overview to determine whether the employees read and accepted the set of rules outlining the responsibilities, ethics, confidentiality and privacy practices by signing the Confirmation of Receipt (CoR) and inspected the EMEA All Mandatory Training Report from Digital University to determine	Deviations noted. *HR EMEA:* For four (4) out of twenty-five (25) randomly selected new DLR EMEA employees, who were hired or transferred during the examination period, we determined per inspection of the Mandatory Policy Attestation overview the employee did not accept the set of rules outlining the responsibilities and ethics and the statement of confidentiality and privacy practices timely upon hire as the employee did not sign the Confirmation of Receipt (CoR) within ninety (90) days post hire in accordance with the Local Recruitment Process Guide. No other deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					whether the employee reaffirmed these annually by completing the mandatory Global Data Privacy training, Information Security training and Insider Trading training. Inspected the notification settings in Digital University to determine whether automated reminders were sent to employees that did not complete the assigned mandatory training.	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CC1.1 - control B**: Hiring procedures include background checks and reference validation, which are performed by HR and retained electronically.	X		Inspected the hiring procedure to determine whether the requirements for background checks and reference validation were included. For a sample of local DLR employees who were either hired or transferred during the examination period, inspected supporting documentation to determine whether a background check and reference validation was performed by local DLR or a third-party agency and retained electronically to enable local DLR to meet the security and availability commitments and requirements.	No deviations noted.
				X	For a sample of DLR EMEA HQ employees who were either hired or transferred during the examination period, inspected supporting documentation to determine whether a background check and reference validation was performed by DLR EMEA or a third-party agency and retained electronically to enable DLR EMEA to meet the security and availability commitments and requirements.	Deviations noted**.** *HR EMEA:* For three (3) out of ten (10) randomly selected new DLR EMEA HQ employees, who were either hired or transferred during the examination period, we were unable to determine whether a background check and reference validation were performed in line with the Global Recruitment Process Guide.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		For one (1) of these new DLR EMEA HQ employees we did not obtain supporting documentation to determine whether a reference validation (of at least two (2) references) was performed in line with the Global Recruitment Process Guide. For two (2) of these new DLR EMEA HQ employees we did not obtain supporting documentation to determine whether a background check was performed in line with the Global Recruitment Process Guide. No other 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**: The Board consists of Directors who qualify as independent under the NYSE listing standards. Such practices and performance against established requirements and expectations are publicly disclosed.		X	Inspected the members of the Board of Directors and the Charter of the Nominating and Corporate Governance Committee of the Board of Directors to determine whether the Board of Directors qualify as independent under the NYSE listing standards and that such practices and performance against established requirements and expectations are publicly disclosed.	No deviations noted.
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**: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed.		X	Inspected the Information Security Manual and organizational charts to determine whether organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. Inspected the latest organizational	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					charts to determine whether organizational charts are available and communicated to employees and updated as needed.	
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 B**: Roles and responsibilities are defined in written job descriptions. The job descriptions are (at least) annually reviewed involving HR and adjusted as needed, which are then electronically stored.	X		For a sample of local DLR employees who were either hired or transferred during the examination period, inspected the function title and related job description to determine whether roles and responsibilities were defined in written job descriptions and were reviewed / updated annually or as needed and observed that the job descriptions are electronically stored.	No deviations noted.
				X	For a sample of DLR EMEA HQ employees who were either hired or transferred during the examination period, inspected the function title and related job description to determine whether roles and responsibilities were defined in written job descriptions and were reviewed / updated annually or as needed and observed that the job descriptions are electronically stored.	No deviations noted.
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**: New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.		X	Inspected the hiring procedure to determine whether guidelines on the hiring process are documented and include verification that the candidates possess the required qualifications to perform the duties as outlined in the job description. For a sample of DLR EMEA HQ employees who were either hired or transferred during the examination period, inspected the HR evaluation as performed on the candidates' qualifications to determine whether the candidates possess the required	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					qualifications to perform the duties as outlined in the job description.	
			X		For a sample of local DLR employees who were either hired or transferred during the examination period, inspected the HR evaluation as performed on the candidates' qualifications to determine whether the candidates possess the required qualifications to perform the duties as outlined in the job description.	No deviations noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CC1.4 - control B**: Training courses are available to new and existing employees to maintain and advance the skill level of personnel.		X	Observed the training platform Digital University and inspected the EMEA All Mandatory Training Report to determine whether training courses are available to new and existing employees to maintain and advance the skill level of personnel.	No deviations noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CC1.4 - control C**: Management evaluates, on an (at least) annual basis, the need for additional resources in order to achieve business objectives.		X	Inspected the documented annual EMEA Headcount Request to determine whether management as evaluated the need for additional resources in order to achieve business objectives.	No deviations noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CC1.4 - control D**: On an annual basis all employees are subject to a performance evaluation to review achievement of objectives and personal development plans.		X	For a sample of DLR EMEA employees, inspected the Goals Detail report from Digital University to determine whether objectives and personal development plans were specified and achievements of objectives and personal development plans were reviewed as part of the annual performance evaluation.	No deviations noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their	**CC1.5 - control A**: Responsibilities and accountability related to the management of internal controls are	X	X	Inspected relevant security documentation, availability procedures and other system	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	internal control responsibilities in the pursuit of objectives.	defined in local and company level policies and procedures.			requirement documentation to determine whether the responsibilities and accountability related to the management of internal controls were defined in local and company level policies and procedures.	

4.6. Criteria related to Communication and Information

Ref	Trust Service Criteria	Control specified by DLR	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**: Based on changes in internal and external context the risks to organisation are monitored and recorded. Based on changes in risks, internal control framework shall be reviewed and updated.		X	Inquired of management and inspected the assessment of the internal control framework and the GRC software tool reports to determine whether the annual assessment by DLR EMEA's Quality Management, of the required (quality) information to support the functioning of the internal control, has been performed. Inspected the assessment of the internal control framework and review evaluation documentation to determine whether, based on changes in internal and external context, the risks to the organisation are monitored and recorded and internal controls are reviewed and updated.	No deviations noted.
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 B**: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. Refer to CC1.3 control A		X	Inspected the Information Security Manual and organizational charts to determine whether organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. Inspected the latest organizational charts to determine whether organizational charts are available and communicated to employees and updated as needed.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	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 A**: Employees are required to complete security awareness training upon hire and annually, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	X		Inquired of management to determine whether training on security awareness and organizational policies and procedures were provided to local DLR employees. Inspected the attendance lists or completion reports and training documentation to determine whether local DLR employees have attended the (local) training on security awareness and organizational policies and procedures that are relevant for their job function. Inspected supporting evidences and inquired of management to determine whether, in case local DLR employees did not attend (local) training on security awareness, follow-up actions were performed and additional training sessions were held to ensure local employees of DLR received awareness training, if possible.	No deviations noted.
				X	Inspected the Acceptable Use Policy to determine whether information security commitments were included. Inquired of management to determine whether training on security awareness was provided to DLR EMEA employees. For a sample of DLR EMEA employees and contractors with access to organisational information assets, inspected the Acceptable Use Policy registration documentation to determine whether personnel has read and accepted their obligations and responsibilities to comply with the	Deviations noted**.** *HR EMEA:* For two (2) out of twenty-five (25) randomly selected new DLR EMEA employees, we determined per inspection of the EMEA Mandatory Training overview that the Security Awareness training was completed more than 90 days post hire. As such, we determined that the security awareness training was not completed timely upon hire in accordance with the Local Recruitment Process Guide. No other deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					corporate and business unit security policies, and determined that monitoring by management was performed and followed-up accordingly with the local DLR entity if necessary. For a sample of DLR EMEA employees who were either hired or transferred during the examination period, inspected the EMEA All Mandatory Training Report from Digital University to determine whether the employee received security awareness training timely upon hire in accordance with the Local Recruitment Process Guide, to understand their obligations and responsibilities to comply with the corporate and business unit security policies. For a sample of existing DLR EMEA employees, inspected the EMEA All Mandatory Training Report from Digital University to determine whether the employee received security awareness training on (at least) an annual basis to determine whether the employee received security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies. Inspected supporting evidences and inquired of management to determine whether, in case DLR EMEA employees did not attend training on	

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					security awareness, follow-up actions were performed. Inspected the notification settings in Digital University to determine whether automated reminders were sent to employees that did not complete the assigned mandatory training.	
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 B**: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the GRC tooling.		X	Inspected the Information Security Manual and the relevant security and availability policies and procedures to determine whether responsibilities of internal personnel were defined. Inspected the GRC tooling to determine whether the relevant security and availability policies and procedures were published and accessible to the internal personnel.	No deviations noted.
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 C**: Documented escalation procedures for reporting security and availability incidents are provided to internal users to guide users in identifying, reporting, and remediating failures, incidents, concerns and other complaints.	X		Inspected the local escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints.	No deviations noted.
				X	Inspected the relevant escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints. Inspected the GRC tooling to determine whether local escalation procedures for reporting security and availability incidents were published	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					and accessible to the internal personnel.	
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**: Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. The organizational charts are available and communicated to employees and updated as needed. Refer to CC1.3 - control A		X	Inspected the Information Security Manual and organizational charts to determine whether organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. Inspected the latest organizational charts to determine whether organizational charts are available and communicated to employees and updated as needed.	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**: DLR informs relevant external stakeholders (vendors and suppliers) about the internal control environment by communicating DLR's requirements (House rules and Terms & Conditions for contractors and Non-disclosure agreements (NDA's). Vendors and suppliers in scope are those who maintain critical infrastructure as detailed in A1.2 - control A, plus the Security Service provider(s) and Security Systems provider(s) / contractor(s).		X	Inspected the DLR EMEA Corporate Procurement Policy, Supplier policy, House rules and Terms & Conditions for contractors and Non-disclosure agreement (NDA) to determine whether DLR EMEA has defined and documented which suppliers were considered 'relevant' and whether DLR EMEA's requirements and communication to relevant external stakeholders (vendors and suppliers) were defined.	No deviations noted.
			X		For a sample of relevant external stakeholders (vendors and suppliers who maintain critical infrastructure or the security systems and / or provide security services), inspected the signed House rules and Terms & Conditions for contractors and Non-disclosure agreements to determine whether DLR EMEA's requirements	No deviations noted. For one (1) out of five (5) randomly selected relevant external stakeholders we determined that a Non-disclosure agreement (NDA) was not available for the full examination period.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					were communicated and confirmed by the relevant external stakeholders.	Per inspection of the Non-disclosure agreement (NDA) we determined that it was signed during the examination period (on May 11, 2022). Per inspection of the contract between the external stakeholder and Interxion Deutschland GmbH, which was signed in June 2018, we determined that the information shared by Interxion Deutschland GmbH with the external stakeholder was not considered confidential, unless specifically mentioned, and therefore Interxion Deutschland GmbH concluded that no NDA was required.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CC2.3 - control B**: The formally documented customer system requirements are communicated to internal users by the Design Transition team at the time of contract signature or when revised as applicable and are documented in the handover overview documentation.	X		For a sample of new local DLR customers and contract renewals during the examination period, inspected the ticket documentation, handover documentation and e-mail communication from the Design Transition team, to determine whether the customer system requirements were documented in the handover overview documentation upon signing of the (initial / renewed / revised) contract and communicated to internal users.	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 C**: Customers receive a standard introductory welcome pack containing key information around the data centre facility responsibilities. The Service Level Agreement, which includes DLR's responsibilities, is communicated to customers upon signing the initial contract.		X	Inspected the introductory welcome pack to determine whether the document contained key information around the data centre facility responsibilities. Inspected the Service Level Agreement (SLA) to determine whether DLR EMEA's responsibilities were included.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
			X		Inspected the DLR EMEA Customer Portal to determine whether the welcome pack is published and available to local DLR customers. For a sample of new local DLR customers, inspected the invite to the Customer Portal to determine the customer was invited to the Customer Portal where the welcome pack is published. For a sample of new local DLR customers, inspected the communication of the SLA to determine whether the SLA was communicated to the customer upon signing the initial contract.	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 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.		X	Inspected the most recent version of the welcome pack to determine whether customer responsibilities, including responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for reporting, were described.	No deviations noted.

4.7. Criteria related to Risk Assessment

Ref	Trust Service Criteria	Control specified by DLR	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**: Management holds an annual company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.		X	Inquired of management and inspected the meeting invite and content of the annual EMEA all hands call to determine whether management holds an annual company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	No deviations noted.
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 B**: Assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	X	X	Inspected the risk management procedures and the annual risk assessments to determine whether assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process.	No deviations noted.
				X	For a sample of risks above the tolerable threshold, inspected risk mitigation plans to determine whether the control activities were documented within the mitigation plans.	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 risks should be managed.	**CC3.2 - control A**: Risk mitigation policies and procedures are in place to guide personnel in the development and deployment of risk mitigation strategies.	X	X	Inquired of management and inspected the risk management procedures to determine whether risk mitigation policies and procedures to guide personnel in the development and deployment of risk mitigation strategies are defined. Inspected the annual risk assessments to determine whether risks were evaluated and risk mitigation strategies were developed and deployed in line with the risk management procedures.	No deviations noted.
CC3.2	COSO Principle 7: The entity identifies risks to	**CC3.2 - control B**: A business recovery plan is in place for each data	X		Inspected the business recovery plans for the data centres in scope to	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.	centre and is reviewed annually by local management.			determine whether the business recovery plans were in place and annually reviewed by DLR's local management.	
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 risks should be managed.	**CC3.2 - control C**: Assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. Refer to CC3.1 - control B	X	X	Inspected the risk management procedures and the annual risk assessments to determine whether assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process.	No deviations noted.
				X	For a sample of risks above the tolerable threshold, inspected risk mitigation plans to determine whether the control activities were documented within the mitigation plans.	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 risks should be managed.	**CC3.2 - control D**: On a (at least a) quarterly 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.		X	Inquired of management to determine whether (at least) on a quarterly 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. For a sample of weeks, inspected the meeting documentation of the Operational Management meetings to determine whether the 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 were discussed.	No deviations noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in	**CC3.3 - control A**: Security stakeholders perform a risk assessment on an annual basis that		X	Inspected the risk management procedures to determine whether the risk of fraud within its business and	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	assessing risks to the achievement of objectives.	considers the potential for fraud. This includes an evaluation of the Fraud Risk Triangle components (pressures, opportunities, and rationalisation) as well as introduced from the use of IT and access to information			documents was identified in the risk register, risk assessment plans and risk assessments. Inquired of management and inspected the annual Enterprise Risk Assessment and DLR EMEA Fraud Risk Assessment Memo to determine whether security stakeholders performed a risk assessment that considers the potential for fraud and include an evaluation of the Fraud Risk Triangle components (pressures, opportunities, and rationalisation) and the use of IT and access to information.	
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CC3.4 - control A**: DLR'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 DLR 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	X	X	Inquired of DLR EMEA's Quality Management and inspected risk management procedures to determine whether the assessment of changes, that could significantly impact the system of internal controls has been defined as part of the risk management procedures. 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 DLR EMEA Risk Management process.	No deviations noted.

4.8. Criteria related to Monitoring Activities

Ref	Trust Service Criteria	Control specified by DLR	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**: The local Operations team reviews DLR's system capacity, availability and security performance on a monthly basis. Corrections and other necessary actions are taken when issues are identified.	X		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 for the issues identified by DLR's local Operations team.	No deviations noted.
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 B**: Documented escalation procedures for reporting security and availability incidents are provided to internal users to guide users in identifying, reporting, and remediating failures, incidents, concerns and other complaints. Refer to CC2.2 - control C	X		Inspected the local escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints.	No deviations noted.
				X	Inspected the relevant escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints. Inspected the GRC tooling to determine whether local escalation procedures for reporting security and availability incidents were published and accessible to the internal personnel.	No deviations noted.
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components	**CC4.1 - control C**: There is (at least) a quarterly meeting with the data centre operation managers and the VP Operations Support EMEA to identify and address potential impairments to the entity's ongoing ability to achieve its objectives. If		X	Inquired of management to determine whether quarterly meetings were scheduled between the Operations Managers and the Vice President Operations Support EMEA to identify and address potential impairments to the entity's ongoing ability to achieve	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	of internal control are present and functioning.	impairments are identified specific projects are set up to resolve those.			its objectives and, if impairments were identified, specific projects were set up to resolve those impairments. For a sample of quarters, inspected the meeting documentation of the operational management meeting to determine whether potential impairments, to DLR EMEA's ongoing ability to achieve its objectives, were identified and follow up actions were initiated to resolve those.	
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 D**: Penetration tests are conducted by accredited independent third party assessor on an annual basis. The results of the audits are reviewed by management as part of the annual risk assessments process.		X	Inspected the penetration test report to determine whether an annual penetration test has been conducted by an accredited independent third party assessor on an annual basis. Inspected ServiceNow ticket(s) to determine that the results of the audits were reviewed by management as part of the annual risk assessments process 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 board of directors, as appropriate.	**CC4.2 - control A**: The local Operations team reviews DLR's system capacity, availability and security performance on a monthly basis. Corrections and other necessary actions are taken when issues are identified. Refer to CC4.1 - control A	X		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 for the issues identified by DLR's local Operations team.	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	**CC4.2 - control B**: The Board consists of Directors who qualify as independent under the NYSE listing standards. Such practices and performance against established requirements and expectations are		X	Inspected the members of the Board of Directors and the Charter of the Nominating and Corporate Governance Committee of the Board of Directors to determine whether the Board of Directors qualify as	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	taking corrective action, including senior management and the board of directors, as appropriate.	publicly disclosed. Refer to CC1.2 - control A			independent under the NYSE listing standards and that such practices and performance against established requirements and expectations are publicly disclosed.	
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 board of directors, as appropriate.	**CC4.2 - control C**: There is (at least) a quarterly meeting with the data centre operation managers and the VP Operations Support EMEA 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		X	Inquired of management to determine whether quarterly meetings were scheduled between the Operations Managers and the Vice President Operations Support EMEA 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 impairments. For a sample of quarters, inspected the meeting documentation of the operational management meeting to determine whether potential impairments, to DLR EMEA's ongoing ability to achieve its objectives, were identified and follow up actions were initiated to resolve those.	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 board of directors, as appropriate.	**CC4.2 - control D**: Penetration tests are conducted by accredited independent third party assessor on an annual basis. The results of the audits are reviewed by management as part of the annual risk assessments process. Refer to CC4.1 - control D		X	Inspected the penetration test report to determine whether an annual penetration test has been conducted by an accredited independent third party assessor on an annual basis. Inspected ServiceNow ticket(s) to determine that the results of the audits were reviewed by management as part of the annual risk assessments process and follow-up actions were documented.	No deviations noted.

4.9. Criteria related to Control Activities

Ref	Trust Service Criteria	Control specified by DLR	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**: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the GRC tooling. Refer to CC2.2 - control B		X	Inspected the Information Security Manual and the relevant security and availability policies and procedures to determine whether responsibilities of internal personnel were defined. Inspected the GRC tooling to determine whether the relevant security and availability policies and procedures were published and accessible to the internal personnel.	No deviations noted.
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 B**: Assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. Refer to CC3.1 - control B	X	X	Inspected the risk management procedures and the annual risk assessments to determine whether assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process.	No deviations noted.
				X	For a sample of risks above the tolerable threshold, inspected risk mitigation plans to determine whether the control activities were documented within the mitigation plans.	No deviations noted.
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 C**: Risk mitigation policies and procedures are in place to guide personnel in the development and deployment of risk mitigation strategies. Refer to CC3.2 - control A	X	X	Inquired of management and inspected the risk management procedures to determine whether risk mitigation policies and procedures to guide personnel in the development and deployment of risk mitigation strategies are defined. Inspected the annual risk assessments to determine whether risks were evaluated and risk mitigation strategies were developed and deployed in line with the risk management procedures.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	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**: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the GRC tooling. Refer to CC2.2 - control B		X	Inspected the Information Security Manual and the relevant security and availability policies and procedures to determine whether responsibilities of internal personnel were defined. Inspected the GRC tooling to determine whether the relevant security and availability policies and procedures were published and accessible to the internal personnel.	No deviations noted.
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 B**: Penetration tests are conducted by accredited independent third party assessor on an annual basis. The results of the audits are reviewed by management as part of the annual risk assessments process. Refer to CC4.1 - control D		X	Inspected the penetration test report to determine whether an annual penetration test has been conducted by an accredited independent third party assessor on an annual basis. Inspected ServiceNow ticket(s) to determine that the results of the audits were reviewed by management as part of the annual risk assessments process and follow-up actions were documented.	No deviations noted.
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 C**: Risk mitigation policies and procedures are in place to guide personnel in the development and deployment of risk mitigation strategies. Refer to CC3.2 - control A	X	X	Inquired of management and inspected the risk management procedures to determine whether risk mitigation policies and procedures to guide personnel in the development and deployment of risk mitigation strategies are defined. Inspected the annual risk assessments to determine whether risks were evaluated and risk mitigation strategies were developed and deployed in line with the risk management procedures.	No deviations noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control	**CC5.2 - control D**: Assigned risk owners select and develop control activities to mitigate the risk identified	X	X	Inspected the risk management procedures and the annual risk assessments to determine whether	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	activities over technology to support the achievement of objectives.	during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. Refer to CC3.1 - control B			assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process.	
				X	For a sample of risks above the tolerable threshold, inspected risk mitigation plans to determine whether the control activities were documented within the mitigation plans.	No deviations noted.
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 E**: 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) - Security staff on site 24 / 7 Annual audits are performed on physical security of the data centre. Refer to CC6.4 - Control B	X		Inquired of management, inspected supporting documentation and observed the data centres in scope to determine whether the required security measures were present. Inspected the annual physical security audit report for the data centres in scope to determine whether a physical security audit has been performed in the examination period.	No deviations noted.
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 related to the management of internal controls are defined in local and company level policies and procedures. Refer to CC1.5 - control A	X	X	Inspected relevant 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 in local and company level policies and procedures.	No deviations noted.
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 B**: Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the GRC		X	Inspected the Information Security Manual and the relevant security and availability policies and procedures to determine whether responsibilities of internal personnel were defined. Inspected the GRC tooling to determine whether the relevant	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		tooling. Refer to CC2.2 - control B			security and availability policies and procedures were published and accessible to the internal personnel.	
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 C**: Documented escalation procedures for reporting security and availability incidents are provided to internal users to guide users in identifying, reporting, and remediating failures, incidents, concerns and other complaints. Refer to CC2.2 - control C	X		Inspected the local escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints.	No deviations noted.
				X	Inspected the relevant escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints. Inspected the GRC tooling to determine whether local escalation procedures for reporting security and availability incidents were published and accessible to the internal personnel.	No deviations noted.
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 D**: Assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold. Refer to CC3.1 - control B	X	X	Inspected the risk management procedures and the annual risk assessments to determine whether assigned risk owners select and develop control activities to mitigate the risk identified during the annual risk assessment process.	No deviations noted.
				X	For a sample of risks above the tolerable threshold, inspected risk mitigation plans to determine whether the control activities were documented within the mitigation plans.	No deviations noted.

4.10. Criteria related to Logical and Physical Access Controls

Ref	Trust Service Criteria	Control specified by DLR	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**: The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements as defined in the Global Password Management Policy. In case passwords requirements cannot be met due technical limitations within the applications, a Risk Acceptance Form (RAF) is available and renewed on an annual basis.	X		Inspected the Global Password Management Policy to determine whether minimum password requirements are defined. For in-scope applications inspected user account listings and authentication settings to determine whether users are required to authenticate with a unique user account, and whether predefined user account and minimum password requirements were enforced as defined in the Global Password Management Policy. For in-scope applications, which cannot comply with the minimum password requirements as defined in the Global Password Management Policy due to technical limitations within the applications, inspected a Risk Acceptance Form (RAF) and determined that the form was approved during the examination period.	No deviations noted.
				X	Inspected the Global Password Management Policy to determine whether minimum password requirements are defined. For in-scope applications inspected user account listings and authentication settings to determine whether the submission of a password and separate user ID was required to access these applications and password requirements were	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					implemented in accordance with the Global Password Management Policy. For in-scope applications, which cannot comply with the minimum password requirements as defined in the Global Password Management Policy due to technical limitations within the applications, inspected a Risk Acceptance Form (RAF) and determined that the form was approved during the examination period.	
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 B**: When possible predefined security groups are utilised to assign role-based access privileges and segregated access to data to the in-scope systems. Refer to CC6.3 - control B	X	X	Inspected authorization listings and authorization matrices to determine whether authorizations were assigned to predefined security groups to segregate access to data for in scope systems. For a sample of new and modified access assigned to internal and external users during the examination period, inspected the supporting documentation to determine whether role-based authorizations based on predefined security groups were assigned to segregate access to data to the in-scope systems in accordance with the logical access procedure.	No deviations noted.
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 C**: External points of connectivity are protected by a firewall complex and an Intrusion Prevention System. In case a firewall configuration needs to be changed or a new firewall needs to be created, it needs to be requested via ServiceNow and approved by the GlobalICT NetEng CAB and GlobalICT		X	Inspected the Information Security Policy and Manual and supporting documentation to determine whether the external points of connectivity to the DLR EMEA environment were protected by a firewall complex and an Intrusion Prevention System (IPS). Inspected all firewall rule (creation / modification) requests in ServiceNow and determined that all completed	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		SecurityCompliance CAB. Refer to CC6.6 - control A			requests were approved by the GlobalICT NetEng CAB and GlobalICT SecurityComplianceCAB.	
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 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 accounts are uniquely identifiable, while application generic accounts are in place if required. Two factor authentication is used for external access to the DLR EMEA network. In case generic accounts are required, mitigating measures (regular account review, password resets and / or password management tooling) are defined and implemented.	X		Inspected the relevant logical access policies and procedures to determine whether a process, on identifying and authenticating users, is formalized. For in-scope applications inspected user account listings and authentication settings to determine whether user accounts on the DLR EMEA network 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, we inspected Risk Acceptance Forms (RAF), account review documentation, password resets and / or password management tooling to determine whether mitigating measures were defined and implemented.	No deviations noted.
				X	For a sample of database servers inspected the database user account listings to determine whether user accounts on database server level had unique identifiers assigned and password authentication techniques were used to substantiate the claimed identity of a user. Inspected the relevant logical access policies and procedures to determine whether a process, on identifying and authenticating users, is formalized. For in-scope applications inspected user account listings and	Deviations noted. *IT EMEA:* For two (2) out of twenty-five (25) randomly selected database servers we determined that no mitigating measures (regular account review, password resets and / or password management tooling), related to the use of generic accounts, were implemented. For one (1) of these database servers we determined that the SA account was disabled on November 1, 2022.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					authentication settings to determine whether user accounts on the DLR EMEA network 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, we inspected Risk Acceptance Forms (RAF), account review documentation, password resets and / or password management tooling to determine whether mitigating measures were defined and implemented. Inspected authentication tools and observed the use of two factor authentication to determine whether two-factor authentication is used for external access to the DLR EMEA network.	For one (1) of these database servers we determined that the SA account was enabled throughout the entire examination period. Per inquiry with the Manager Internal Control DLR EMEA we determined that the SA account could not be disabled, due to technical limitations. 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.	X		Inspected the user registration policies and procedures to determine whether the user registration and de-registration procedure is formalized. For a sample of new and modified access assigned to internal and external users to local applications granted during the examination period, inspected the ServiceNow ticket documentation to determine whether the request was recorded and approved by appropriate management, and the granted access and authorizations match the requested access and authorizations. For a sample of local DLR employees and external contractors with access	Deviations noted. *User registration:* For one (1) of the six (6) randomly selected new and modified access, assigned to internal and external users to in-scope local Interxion Deutschland GmbH applications or Active Directory groups, providing access to local Interxion Deutschland GmbH applications, we were unable to determine that an authorized access request was available for assigning access to one (1) Active Directory group. Per inspection of the joiner form, for the new access assigned, we determined that access to the Active

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					to IT assets who left the local DLR organization during the examination period, inspected supporting documentation to determine whether access was revoked to the DLR EMEA network and the in scope local applications (if required) in a timely manner.	Directory group was authorized based on the function of the user. *User deregistration:* For three (3) out of fifteen (15) randomly selected Interxion Deutschland GmbH employees and external contractors with access to IT assets, who left the organization during the examination period, we determined that the Active Directory account was disabled after the leave date. We determined, for each of these three (3) selected leavers, that the Active Directory account was not used or could not be used to log-in after the leave date and that the selected leaver did not have access to the local applications in scope. No other deviations noted.
				X	Inspected the user registration policies and procedures to determine whether the user registration and de-registration procedure is formalized. For a sample of new and modified access assigned to internal and external users to ServiceNow, Ultimo and Customer Portal during the examination period, inspected the ServiceNow ticket documentation to determine whether the request was recorded and approved by appropriate management, and the granted access and authorizations match the requested access and authorizations. For a sample of DLR EMEA	Deviations noted. *IT EMEA (Ultimo user registration):* For three (3) out of twenty-five (25) randomly selected Ultimo authorization changes we determined that the formal user registration procedure has not been followed for granting authorization for these users. For two (2) out of the three (3) accounts we determined that access was 'granted' (not removed) based on access revocation requests. For one (1) out of the three (3) account we determined that account was created based on an authorized request, but an incorrect group was assigned.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					employees and external contractors with access to IT assets who left the DLR EMEA organization during the examination period, inspected the supporting documentation to determine whether access was revoked to the DLR EMEA network and the relevant HQ applications ServiceNow, Ultimo and / or Customer Portal in a timely manner.	Additional procedures performed: For all three (3) accounts we determined that the accounts were not used after their access should have been removed or was incorrectly created. *IT EMEA (User deregistration):* For three (3) out of nine (9) randomly selected DLR EMEA employees and external contractors with access to IT assets who left the organization during the examination period we determined that the Active Directory account and applications in scope (Ultimo and ServiceNow) were disabled after the leave date or not disabled at all. Additional procedures performed: For two (2) of these selected leavers we determined that the Activity Directory accounts were not used anymore after the leave date. For one (1) of these selected leavers we determined per inspection of the Active Directory logging, that the account was disabled after six (6) weeks, and therefore the leaver was not able to login anymore after six (6) weeks. 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	**CC6.2- control B**: For in-scope business critical applications, users access reviews are performed on an annual basis to ensure that access to data was restricted to authorised personnel and provided for segregation of duties.	X	X	Inspected the logical access policies and procedures to determine whether a management review process, on users' access rights and privileged access, is formalized.	Deviations noted. *Interxion Deutschland GmbH:* For one (1) out of seven (7) in-scope local applications (BVMS) we determined that the users, which are authorized via the Active Directory to

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Refer to CC6.3 - control A			Inspected the management review documentation to determine whether the management review, on users' access rights and privileged access, was performed on complete and accurate user overviews on at least annual basis for the in scope applications (software) in accordance with the logical access policies and procedures to ensure that access to data was restricted to authorised personnel and provided for segregation of duties. 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 completed.	this application, were not included in the user list that was used for the performed annual management review. *IT EMEA (Customer Portal):* Per inspection of the annual Customer Portal user access review we were unable to determine that all accounts and related authorizations were included in the user access review. *IT EMEA (Ultimo):* For the performed annual review on the Ultimo authorizations, we determined that the review for HQ accounts was not correctly performed, as an employee who left the DLR EMEA organization during the examination period (CC6.2 - control A) was not detected as part of the subsequent annual review. No other deviations noted.
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**: For in-scope business critical applications, users access reviews are performed on an annual basis to ensure that access to data was restricted to authorised personnel and provided for segregation of duties.	X	X	Inspected the logical access policies and procedures to determine whether a management review process, on users' access rights and privileged access, is formalized. Inspected the management review documentation to determine whether the management review, on users' access rights and privileged access, was performed on complete and accurate user overviews on at least annual basis for the in scope applications (software) in accordance with the logical access policies and procedures to ensure that access to	Deviations noted. *Interxion Deutschland GmbH:* For one (1) out of seven (7) in-scope local applications (BVMS) we determined that the users, which are authorized via the Active Directory to this application, were not included in the user list that was used for the performed annual management review. *IT EMEA (Customer Portal):* Per inspection of the annual Customer Portal user access review we were unable to determine that all

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					data was restricted to authorised personnel and provided for segregation of duties. 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 completed.	accounts and related authorizations were included in the user access review. *IT EMEA (Ultimo):* For the performed annual review on the Ultimo authorizations, we determined that the review for HQ accounts was not correctly performed, as an employee who left the DLR EMEA organization during the examination period (CC6.2 - control A) was not detected as part of the subsequent annual review. No other deviations noted.
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 B**: When possible predefined security groups are utilised to assign role-based access privileges and segregated access to data to the in-scope systems.	X	X	Inspected authorization listings and authorization matrices to determine whether authorizations were assigned to predefined security groups to segregate access to data for in scope systems. For a sample of new and modified access assigned to internal and external users during the examination period, inspected the supporting documentation to determine whether role-based authorizations based on predefined security groups were assigned to segregate access to data to the in-scope systems in accordance with the logical access procedure.	No deviations noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the	**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 information systems and services.	X		Inspected the user registration policies and procedures to determine whether the user registration and de-registration procedure is formalized. For a sample of new and modified access assigned to internal and	Deviations noted. *User registration:* For one (1) of the six (6) randomly selected new and modified access, assigned to internal and external users to in-scope local Interxion

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Refer to CC6.2 - control A			external users to local applications granted during the examination period, inspected the ServiceNow ticket documentation to determine whether the request was recorded and approved by appropriate management, and the granted access and authorizations match the requested access and authorizations. For a sample of local DLR employees and external contractors with access to IT assets who left the local DLR organization during the examination period, inspected supporting documentation to determine whether access was revoked to the DLR EMEA network and the in scope local applications (if required) in a timely manner.	Deutschland GmbH applications or Active Directory groups, providing access to local Interxion Deutschland GmbH applications, we were unable to determine that an authorized access request was available for assigning access to one (1) Active Directory group. Per inspection of the joiner form, for the new access assigned, we determined that access to the Active Directory group was authorized based on the function of the user. *User deregistration:* For three (3) out of fifteen (15) randomly selected Interxion Deutschland GmbH employees and external contractors with access to IT assets, who left the organization during the examination period, we determined that the Active Directory account was disabled after the leave date. We determined, for each of these three (3) selected leavers, that the Active Directory account was not used or could not be used to log-in after the leave date and that the selected leaver did not have access to the local applications in scope. No other deviations noted.
				X	Inspected the user registration policies and procedures to determine whether the user registration and de-registration procedure is formalized. For a sample of new and modified	Deviations noted. *IT EMEA (Ultimo user registration):* For three (3) out of twenty-five (25) randomly selected Ultimo authorization changes we determined

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					access assigned to internal and external users to ServiceNow, Ultimo and Customer Portal during the examination period, inspected the ServiceNow ticket documentation to determine whether the request was recorded and approved by appropriate management, and the granted access and authorizations match the requested access and authorizations. For a sample of DLR EMEA employees and external contractors with access to IT assets who left the DLR EMEA organization during the examination period, inspected the supporting documentation to determine whether access was revoked to the DLR EMEA network and the relevant HQ applications ServiceNow, Ultimo and / or Customer Portal in a timely manner.	that the formal user registration procedure has not been followed for granting authorization for these users. For two (2) out of the three (3) accounts we determined that access was 'granted' (not removed) based on access revocation requests. For one (1) out of the three (3) account we determined that account was created based on an authorized request, but an incorrect group was assigned. <u>Additional procedures performed</u>: For all three (3) accounts we determined that the accounts were not used after their access should have been removed or was incorrectly created. *IT EMEA (User deregistration):* For three (3) out of nine (9) randomly selected DLR EMEA employees and external contractors with access to IT assets who left the organization during the examination period we determined that the Active Directory account and applications in scope (Ultimo and ServiceNow) were disabled after the leave date or not disabled at all. <u>Additional procedures performed:</u> For two (2) of these selected leavers we determined that the Activity Directory accounts were not used anymore after the leave date. For one (1) of these selected leavers we determined per inspection of the Active Directory logging, that the account was disabled after six (6)

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		weeks, and therefore the leaver was not able to login anymore after six (6) weeks. No other deviations noted.
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 temporary physical access rights to the data centre for visiting contractors and 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	X		Inspected the relevant physical security policies and procedures to determine whether procedures were in place for granting access to the data centre for temporary contractors and visiting customers. Inspected the relevant physical security policies, procedures and supporting documentation 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. Inspected the physical security policies and procedures, the Customer Portal and ServiceNow to determine whether the central temporary physical access rights requests process managed by DLR EMEA's European Customer Service Centre (ECC) was defined and implemented. For a sample of temporary access requests, inspected the ServiceNow request ticket and badge access system entry log to determine whether the request was recorded and authorized by the access authorizer using the Customer Portal, and that the areas entered were included on the list of areas approved for entry in	Deviations noted. For two (2) out of twenty-five (25) randomly selected temporary access requests we determined that access to more footprints (areas) was granted by Interxion Deutschland GmbH than requested by the access authoriser. Per inspection of the badge access log we determined that the additional granted customer footprints were not used by the visitors and the areas were not visited. Per observation on August 29, 2022, we determined that Interxion Deutschland GmbH management has split these access groups to address this issue and to be able to only assign the requested footprints (areas). No other deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					accordance with the relevant physical security policies and procedures.	
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 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) - Security staff on site 24 / 7 Annual audits are performed on physical security of the data centre.	X		Inquired of management, inspected supporting documentation and observed the data centres in scope to determine whether the required security measures were present. Inspected the annual physical security audit report for the data centres in scope to determine whether a physical security audit has been performed in the examination period.	No deviations noted.
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 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 DLR EMEA's European Customer Service Centre (ECC). Access requests are processed according to Customer Change List Authorizer credentials and parameters and assigned to DLR Security at the specific data centre. For DLR employees and third parties: All new, changed or revoked permanent physical access rights are requested by a DLR Change List Authorizer, using a central process managed by DLR EMEA's European Customer Service Centre (ECC). Access is validated and granted by the local Security Manager.	X		Inspected the relevant physical security policies and procedures to determine whether 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, the Customer Portal and ServiceNow to determine whether the central permanent physical access rights requests (new, changed or revoked) process managed by DLR EMEA's European Customer Service Centre (ECC) was defined and implemented. For a sample of granted and changed permanent physical access during the examination period, inspected the ServiceNow request ticket submitted by the Customer or DLR Change List Authorizer, ServiceNow Authorization overview, and badge access profile to determine whether the permanent	Deviations noted. For one (1) out of twenty-five (25) randomly selected granted and changed permanent physical access we determined that access to more customer footprints (areas) was granted than requested. Per inspection of the badge access log we determined that the additional granted customer footprints were not used by the visitor and the areas were not visited. Per observation on December 16, 2022, we determined that Interxion Deutschland GmbH management has split the access group to address this issue and to be able to only assign the requested customer footprints (areas). No other deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					physical access request was recorded, validated by the local Security Manager (for local DLR employees) or Customer Change List Authorizer (for Customers), and access rights assigned in the badge access control system matched the access authorized in ServiceNow. For a sample of requests to revoke permanent physical access during the examination period, inspected the ServiceNow request ticket submitted by the Customer or DLR Change List Authorizer, the badge access profile as well as badge access logs to determine whether requests for revocation of permanent physical access to the data centre were assigned to local DLR Security at the concerned data centre, processed in a timely manner and in accordance with the Customer or DLR Change List Authorizer's request.	
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 D**: Physical access rights for all DLR staff and third parties are reviewed annually to ensure that access rights are accurate, valid and assigned restrictively (least privilege principle).	X		Inspected the relevant physical security policies and procedures to determine whether procedures were in place for reviewing physical access rights. Inspected the annual physical access rights management review to determine whether the granted permanent physical access of local DLR staff and third parties were accurate, valid and assigned restrictively. Inspected the documentation of the annual physical access rights management review to determine	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					whether follow-up actions, resulting from the review on physical access rights for in scope data centres, were completed.	
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 E**: The sharing of access badges and tailgating are prohibited by policy.	X		Inspected the relevant physical security policies and procedures and House rules to determine whether 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 temporary physical access rights to the data centre for visiting contractors and 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	X		Inspected the relevant physical security policies and procedures to determine whether procedures were in place for granting access to the data centre for temporary contractors and visiting customers. Inspected the relevant physical security policies, procedures and supporting documentation 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. Inspected the physical security policies and procedures, the Customer Portal and ServiceNow to determine whether the central temporary physical access rights requests process managed by DLR EMEA's European Customer Service Centre (ECC) was defined and implemented.	Deviations noted. For two (2) out of twenty-five (25) randomly selected temporary access requests we determined that access to more footprints (areas) was granted by Interxion Deutschland GmbH than requested by the access authoriser. Per inspection of the badge access log we determined that the additional granted customer footprints were not used by the visitors and the areas were not visited. Per observation on August 29, 2022, we determined that Interxion Deutschland GmbH management has split these access groups to address this issue and to be able to only assign the requested footprints (areas). No other deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					For a sample of temporary access requests, inspected the ServiceNow request ticket and badge access system entry log to determine whether the request was recorded and authorized by the access authorizer using the Customer Portal, and that the areas entered were included on the list of areas approved for entry in accordance with the relevant physical security policies and procedures.	
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 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) - Security staff on site 24 / 7 Annual audits are performed on physical security of the data centre. Refer to CC6.4 - Control B	X		Inquired of management, inspected supporting documentation and observed the data centres in scope to determine whether the required security measures were present. Inspected the annual physical security audit report for the data centres in scope to determine whether a physical security audit has been performed in the examination period.	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 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 DLR EMEA's European Customer Service Centre (ECC). Access requests are processed according to Customer Change List Authorizer credentials and parameters and assigned to DLR Security at the specific data centre. For DLR employees and third parties:	X		Inspected the relevant physical security policies and procedures to determine whether 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, the Customer Portal and ServiceNow to determine whether the central permanent physical access rights requests (new, changed or revoked)	Deviations noted. For one (1) out of twenty-five (25) randomly selected granted and changed permanent physical access we determined that access to more customer footprints (areas) was granted than requested. Per inspection of the badge access log we determined that the additional granted customer footprints were not used by the visitor and the areas were not visited.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		All new, changed or revoked permanent physical access rights are requested by an DLR Change List Authorizer, using a central process managed by DLR EMEA's European Customer Service Centre (ECC). Access is validated and granted by the local Security Manager. Refer to CC6.4 - control C			process managed by DLR EMEA's European Customer Service Centre (ECC) was defined and implemented. For a sample of granted and changed permanent physical access during the examination period, inspected the ServiceNow request ticket submitted by the Customer or DLR Change List Authorizer, ServiceNow Authorization overview, and badge access profile to determine whether the permanent physical access request was recorded, validated by the local Security Manager (for local DLR employees) or Customer Change List Authorizer (for Customers), and access rights assigned in the badge access control system matched the access authorized in ServiceNow. For a sample of requests to revoke permanent physical access during the examination period, inspected the ServiceNow request ticket submitted by the Customer or DLR Change List Authorizer, the badge access profile as well as badge access logs to determine whether requests for revocation of permanent physical access to the data centre were assigned to local DLR Security at the concerned data centre, processed in a timely manner and in accordance with the Customer or DLR Change List Authorizer's request.	Per observation on December 16, 2022, we determined that Interxion Deutschland GmbH management has split the access group to address this issue and to be able to only assign the requested customer footprints (areas). No other deviations noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover	**CC6.5 - control D**: Physical access rights for all DLR staff and third parties are reviewed annually to ensure that access rights are accurate, valid and assigned	X		Inspected the relevant physical security policies and procedures to determine whether procedures were in place for reviewing physical access rights.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	restrictively (least privilege principle). Refer to CC6.4 - control D			Inspected the annual physical access rights management review to determine whether the granted permanent physical access of local DLR staff and third parties were accurate, valid and assigned restrictively. Inspected the documentation of the annual physical access rights management review to determine whether follow-up actions, resulting from the review on physical access rights for in scope data centres, were completed.	
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 E**: The sharing of access badges and tailgating are prohibited by policy. Refer to CC6.4 - control E	X		Inspected the relevant physical security policies and procedures and House rules to determine whether procedures were in place which prohibit sharing of access badges and tailgating.	No deviations noted.
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. In case a firewall configuration needs to be changed or a new firewall needs to be created, it needs to be requested via ServiceNow and approved by the GlobalICT NetEng CAB and GlobalICT SecurityCompliance CAB.		X	Inspected the Information Security Policy and Manual and supporting documentation to determine whether the external points of connectivity to the DLR EMEA environment were protected by a firewall complex and an Intrusion Prevention System (IPS). Inspected all firewall rule (creation / modification) requests in ServiceNow and determined that all completed requests were approved by the GlobalICT NetEng CAB and GlobalICT SecurityComplianceCAB.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
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**: DLR EMEA 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.		X	Inspected the relevant security policies and procedures to determine whether the process is 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	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 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 accounts are uniquely identifiable, while application generic accounts are in place if required. Two factor authentication is used for external access to the DLR EMEA 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	X		Inspected the relevant logical access policies and procedures to determine whether a process, on identifying and authenticating users, is formalized. For in-scope applications inspected user account listings and authentication settings to determine whether user accounts on the DLR EMEA network 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, we inspected Risk Acceptance Forms (RAF), account review documentation, password resets and / or password management tooling to determine whether mitigating measures were defined and implemented.	No deviations noted.
				X	For a sample of database servers inspected the database user account listings to determine whether user accounts on database server level had unique identifiers assigned and password authentication techniques were used to substantiate the claimed identity of a user.	Deviations noted. *IT EMEA:* For two (2) out of twenty-five (25) randomly selected database servers we determined that no mitigating measures (regular account review, password resets and / or password management tooling), related to the

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					Inspected the relevant logical access policies and procedures to determine whether a process, on identifying and authenticating users, is formalized. For in-scope applications inspected user account listings and authentication settings to determine whether user accounts on the DLR EMEA network 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, we inspected Risk Acceptance Forms (RAF), account review documentation, password resets and / or password management tooling to determine whether mitigating measures were defined and implemented.	use of generic accounts, were implemented. For one (1) of these database servers we determined that the SA account was disabled on November 1, 2022. For one (1) of these database servers we determined that the SA account was enabled throughout the entire examination period. Per inquiry with the Manager Internal Control DLR EMEA we determined that the SA account could not be disabled, due to technical limitations. No other deviations noted.
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 agents are installed on workstations, laptops, and servers supporting such software. For updating the AI engines via releases, test groups are created before the releases are deployed. Devices that haven't been updated are reviewed periodically and follow up actions are taken.		X	Inspected the anti-virus monitoring tool to determine whether workstations, laptops, and systems were monitored to ensure anti-virus software agents were installed. For a sample of releases of anti-virus agent versions to update the AI engines, inspected anti-virus monitoring tool, to determine that test groups are created before the releases are deployed. Inspected supporting documentation to determine that devices are updated automatically and that follow up actions were taken for devices that were not automatically updated.	No deviations noted.

4.11. Criteria related to System Operations

Ref	Trust Service Criteria	Control specified by DLR	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**: A formal threat and vulnerability management process is in place for addressing identified threats and vulnerabilities. Findings are remediated according to internal SLAs.		X	Inspected the policies and procedures regarding scanning and monitoring on vulnerabilities to determine that a formal threat and vulnerability management process for addressing identified threats and vulnerabilities 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 weeks inspected the vulnerability scan reports to determine whether a weekly scan, to detect threats and vulnerabilities to the defined systems, has been performed. Inspected meeting minutes, incident ticket documentation or remediation plans, in case vulnerabilities or unauthorized changes were detected, to determine whether follow-up was performed and documented in incident tickets according to internal SLAs.	Deviations noted. *IT EMEA:* We were unable to determine whether follow-up (according to internal SLA) has been performed for all vulnerabilities and threats which were identified in the weekly Vulnerability Scanning reports as documentation of the follow-up is not available or retained. No other deviations noted.
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	**CC7.1 - control B**: All critical systems are configured according to documented baselines. DLR EMEA performs an annual scan on these systems. In case unauthorized changes are detected, corrective actions are initiated.		X	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 were defined.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	discovered vulnerabilities.				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. Inspected the annual baseline scan results report, to determine whether all critical systems were included in the annual baseline scan and in case exceptions were detected, we determined that corrective actions were initiated.	
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**: Documented escalation procedures for reporting security and availability incidents are provided to internal users to guide users in identifying, reporting, and remediating failures, incidents, concerns and other complaints. Refer to CC2.2 - control C	X		Inspected the local escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints.	No deviations noted.
				X	Inspected the relevant escalation procedures for reporting security and availability incidents to determine whether guidelines were defined for identifying, reporting, and remediating failures, incidents, concerns and other complaints. Inspected the GRC tooling to determine whether local escalation procedures for reporting security and availability incidents were published and accessible to the internal personnel.	No deviations noted.
CC7.2	The entity monitors system components and the operation of those	**CC7.2 - control B**: Any attempt of illegal access to the network is automatically monitored, detected and		X	Inspected monitoring software tools to determine that any attempt of illegal	Deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
	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.	logged. Unauthorised devices are automatically diverted to an isolated VLAN. On a daily basis the functioning of the configuration is monitored. In case the configuration needs to be changed it will be handled via the configuration management process.			access to the network is automatically monitored, detected and logged. Inspected router configurations and router setup templates to determine that unauthorised devices are automatically diverted to an isolated VLAN. Inspected Configuration Monitoring logging to determine that on a daily basis the functioning of the configuration is monitored. Inspected ServiceNow tickets to determine that in case the configuration needs to be changed it will be handled via the configuration management process.	*IT EMEA:* We determined, per inspection of the Configuration Monitoring Log, that during January and February 2022, the functioning of the configuration was not monitored on a daily basis. No other deviations 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.		X	Inspected the relevant incident management policies and procedures to determine whether 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 the security / operations groups were specified 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 to determine whether the defined protocol has been	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					followed for logical security and availability breaches and incidents.	
			X		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, to determine whether the defined protocol has been followed for physical security and availability breaches and incidents.	No deviations 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 B**: Security and availability breaches and incidents, with user or customer impact, are communicated to relevant stakeholders and when required reviewed in bi-weekly MO meetings.	X		For a sample of security and availability breaches and incidents with user or customer impact, inspected communication to determine whether security and availability breaches and incidents were communicated to relevant stakeholders.	No deviations noted.
				X	For a sample of weeks, inspected meeting minutes of the bi-weekly DLR EMEA MO meetings to determine whether security and availability breaches and incidents, with user or customer impact, were reviewed (when required).	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.		X	Inspected the relevant incident management policies and procedures to determine whether 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 the	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		Refer to CC7.3 - control A			security / operations groups were specified 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 to determine whether the defined protocol has been followed for logical security and availability breaches and incidents.	
			X		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, to determine whether the defined protocol has been followed for physical security and availability breaches and incidents.	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 B**: Security and availability breaches and incidents, with user or customer impact, are communicated to relevant stakeholders and when required reviewed in bi-weekly MO meetings. Refer to CC7.3 - control B	X		For a sample of security and availability breaches and incidents with user or customer impact, inspected communication to determine whether security and availability breaches and incidents were communicated to relevant stakeholders.	No deviations noted.
				X	For a sample of weeks, inspected meeting minutes of the bi-weekly DLR EMEA MO meetings to determine whether security and availability breaches and incidents, with user or customer impact, were reviewed (when required).	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	**CC7.5 - control A**: DLR 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.	X		Inquired of local DLR 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. Inspected the annual Business Continuity test report, of the critical environmental protections systems in the data centre, to determine whether local DLR has tested the Business Continuity procedures and Crisis Resolution procedures at least annually.	No deviations noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	**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		X	Inspected the relevant incident management policies and procedures to determine whether 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 the security / operations groups were specified 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 to determine whether the defined protocol has been followed for logical security and availability breaches and incidents.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
			X		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, to determine whether the defined protocol has been followed for physical security and availability breaches and incidents.	No deviations noted.

4.12. Criteria related to Change Management

Ref	Trust Service Criteria	Control specified by DLR	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**: Documented policies and procedures are in place to guide personnel in the change management process.		X	Inspected the relevant change management procedure to determine whether documented policies and procedures are in place to guide personnel in the change management process.	No deviations noted.
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 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, approved and implemented in line with the change management process.	X		For a sample of implemented changes to data centre infrastructure or monitoring systems, inspected the risk assessment in the change ticket to determine whether changes were evaluated to determine the potential impact on security and availability commitments and requirements. For a sample of implemented changes to data centre infrastructure or monitoring systems, inspected the approval flow in the change ticket and the signed-off test plan to determine whether changes are appropriately authorized, approved and implemented in line with the change management procedure.	No deviations noted.
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 C**: During the ongoing risk assessment process and the 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.	X		Inspected DLR's local 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.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					Inspected a local DLR project to determine whether change requests and / or business cases were created for the identified and required changes.	
				X	Inspected the Global ITOE risk assessment and the Global ITOE planning, budgeting process and change ticket 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. Inspected a Global ITOE project to determine whether change requests and / or business cases were created for the identified and required changes.	No deviations noted.
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 D**: Incidents classified by DLR as 'high severity incidents' are managed via the Incident Management Procedure and logged and followed up in ServiceNow. When required corrective actions will be implemented via a Change Request or an Ultimo Work order.	X	X	Inspected the Incident Management Procedure to determine whether documented policies and procedures are in place to guide personnel in the incident management process and criteria have been defined for classifying incidents as 'high severity incidents'. For a sample of incidents classified by local DLR and / or DLR EMEA as 'high severity incidents', inspected the ServiceNow incident ticket, customer notification, incident report, change ticket(s) and / or Ultimo Work order(s) to determine whether incidents are managed via the Incident Management Procedure and logged and followed up in ServiceNow and whether corrective actions (when	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
					required) were implemented via a Change Request or an Ultimo Work order and the incident report was shared with the (potentially) impacted customers.	

4.13. Criteria related to Risk Mitigation

Ref	Trust Service Criteria	Control specified by DLR	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**: DLR'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.	X		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 responsible local DLR management based on identified threats and risk tolerances and to determine whether measures were specified to address the identified risks. Inspected the Business Recovery Plan to determine whether mitigating measures for risks, arising from potential business disruptions, were documented.	No deviations noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CC9.1 - control B**: Risk mitigation policies and procedures are in place to guide personnel in the development and deployment of risk mitigation strategies. Refer to CC3.2 - Control A	X	X	Inquired of management and inspected the risk management procedures to determine whether risk mitigation policies and procedures to guide personnel in the development and deployment of risk mitigation strategies are defined. Inspected the annual risk assessments to determine whether risks were evaluated and risk mitigation strategies were developed and deployed in line with the risk management procedures.	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	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 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	X		Inspected the business recovery plans for the data centres in scope to determine whether the business recovery plans were in place and annually reviewed by DLR's local management.	No deviations noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	**CC9.2 - control A**: DLR EMEA'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.		X	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) surveys and IT Security surveys to determine whether mitigations on identified risks, associated with vendors and business partners, were documented in the risk register, risk assessment plans and risk assessments.	No deviations noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	**CC9.2 - control B**: DLR's management has, on a periodic basis, meetings with key vendors and suppliers to discuss the identified risks and mitigating measures related to external stakeholders. The need and frequency of these periodic meetings is determined on	X	X	Inquired of management and inspected the DLR EMEA Corporate Procurement Policy and (local) supplier policies to determine whether DLR EMEA's requirements on regular meetings with key vendors and suppliers were defined. Inspected the (local) stakeholder	No deviations noted.

Ref	Trust Service Criteria	Control specified by DLR	Scope		Test of Controls performed by EY	Results of Tests
			Local	HQ		
		the impact of key vendors and suppliers on internal controls on security and availability of the data centre operations and documented in the (local) stakeholder overview. Vendors and suppliers in scope are those who maintain critical infrastructure as detailed in A1.2 - control A, plus the Security Service provider(s) and Security Systems provider(s) / contractor(s).			overview on internal controls to determine whether need and frequency of the periodic meetings key vendors and suppliers is documented. For a sample of key vendors and suppliers, inspected the meeting invites, and / or meeting minutes to determine whether meetings were held based on the defined frequency 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. Changes to the 2023 SOC2 report schedule

In 2023 the SOC2 program will be combined with Global DLR, this means that a new audit firm will perform the evaluation. Because of the size of the program and the fact that there will be still evidence being evaluated during January 2024, the 2023 reports will not be available until April 2024.

5.2. Management responses to reported deviations

5.2.1. Management response on the deviation related to CC1.1 - control A:

- Scope: HR EMEA
- Containment: No containment actions needed, for the Mandatory Policy Attestation was performed only not in a timely manner.
- Customer impact: None
- Root Cause Analysis: Mandatory Policy Attestation tasks are not assigned automatically to new employees and contractors. There is a manual action for which a new employee or contractor (external) needs to click on a link from the GRC application (MetricStream) in order to get the task assigned. Once the employee or contractor clicks on the link, the system will send out automatic reminders to complete the attestation. In addition to this, there is a lack of monitoring activity from the HR support team in collaboration with the respective line manager due to lack of awareness and inadequate reports from the GRC application.
- Corrective Action: Project to standardize the process of assigning all new hire attestations to new hires via the global instance of ServiceNow (GSN) in progress and expected to go live by May 2023. This will automate the assignment of the tasks and will allow for a standard reporting and audit process. 2023 new hires through April will still receive the link to MetricStream, and the local HR teams have been trained and communicated to regarding their responsibility of sending the link and following up for completion. The HR Ops team is also conducting regular global audits and following up with Local HR reminding them of their obligation to send the links to new hires.
  Improve on the reporting capabilities of the existing GRC application.
  Additional monitoring activities to be performed through control testing and through quarterly reviews of the control performance by the Quality manager in collaboration with the HR Ops team.
  - Status: In progress

5.2.2. Management response on the deviation related to CC1.1 - control B:

- Scope: HR EMEA
- Containment: Background- and Reference checks were done retrospectively, and training was given to all local HR and Talent Acquisition teams on Recruitment process and responsible task owners.
- Customer Impact: None

- Root Cause Analysis: In EMEA Background checks are conducted primarily by HR Business Partners (HRBPs). Reference checks are conducted by either Recruiters or HRBP's depending on the country. With a significant number of new employees and contractors in both the Recruitment and the HR teams, there have been some gaps with regard to training new personnel on who is responsible in each country to carry out both background checks and reference checks and the quality of the checks required (including escalation processes when checks cannot be completed). Background and reference checks are currently carried out to different standards depending on the country of hire. This includes the varying use of 3rd party suppliers (such as HireRight) and DLR employees to conduct checks. The lack of consistency across borders in EMEA adds to the uncertainty on approach and quality of checks required.
- Corrective Action: The consistency challenges noted above has prompted HR to conduct a full review of the background check / reference checking processes. The goal is to move to a more consistent process across EMEA with an effective 3rd party supplier. In the meantime, the following measures will take place:
    1. HR Ops to confirm who is responsible country by country for both background checks and references (RACI). Communication to be sent to HR and Recruitment staff across EMEA as a reminder.
    2. HR Ops to identify any training gaps and ensure this is closed out with training events. This information will be included as part of the induction training for any new HR or new Recruitment team members.
    3. Managers of HR and Recruitment personnel executing background check / reference check activities to cascade and monitor performance.
    4. HR Ops to carry out monthly performance checks to stay on top of any issues. This will be a combination of auditing progress centrally through data (pan EMEA) and Recruitment Team Leaders monitoring their own teams on 121's.
    5. Additional monitoring activities to be performed through control testing and through quarterly reviews of the control performance by the local Quality managers in collaboration with the local HR / Recruitment team.
        - Status: In progress

5.2.3. Management response on the deviation related to CC2.2 - control A:

- Scope: HR EMEA
- Containment: No containment actions needed, for the Security Awareness Training was performed only not in a timely manner.
- Customer Impact: No
- Root Cause Analysis: No timely follow-up was given by the new hire's line manager, even though the application where training is performed sends out multiple reminders to the new hire with line manager in copy. Lack of monitoring by local HR due personnel changes.
- Corrective Action: Local HR team informed about the process. HR Ops team to conduct regular global audits and following up with local HR.
- Additional monitoring activities to be performed through control testing and through quarterly reviews of the control performance by the Quality manager in collaboration with the local HR team.
    - Status: In progress

5.2.4. Management response on the deviation related to CC6.1 - control D:

- Scope: IT EMEA
- Containment: Database Server is in segmented and restricted access network area
- Customer Impact: None

- Root Cause Analysis: Disabling the SA account led to unforeseen operational disturbance, resulting in re-activation of generic account.
- Corrective Action:
    - Status: Cannot be resolved. Vendor assistance not determined what's causing the issue. Account cannot be disabled.

5.2.5. Management response on deviation related to CC6.2 - control A:

- Scope: IT EMEA
- Containment: Application Access is only possible using Enabled Active Directory accounts
- Customer Impact: None
- Root Cause Analysis: Due to disturbance / de-activation of formal JML processing combined with change in identity registration as result of integration activity registration and de-registration occurred manually.
- Corrective Action:
    - Status: Resolved
    - JML process has been repaired and identity registration has been aligned.

5.2.6. Management response on deviation related to CC6.2 - control A:

- Scope: Local (user registration)
- Containment: All individuals are being registered with new accounts. A re-use of already created accounts is no longer allowed.
- Customer Impact: None
- Root Cause Analysis: Re-usage of a revoked account for a new hired employee by HR resulted in an intermixing of account rights.
- Corrective Action: Guidelines given to HR to no longer re-use previously created accounts; revoked accounts shall be blocked (via blacklist)
    - Status: Resolved

- Scope: Local (user de-registration)
- Containment: Access rights being terminated will be disabled for the next business day, by a prioritised "Revoke Access" process.
- Customer Impact: None
- Root Cause Analysis: The normal ticketing process to revoke user access takes too long as it is dependent on HR / IT processing the revoke access ticket.
- Corrective Action: The priority "Revoke Access" is being used to terminate access rights within 24 business hours
    - Status: Resolved

5.2.7. Management response on deviation related to CC6.3 - control A:

- Scope: IT EMEA
- Containment: The users list from Interxion AD was compared with the one extracted from DLR AD and Azure, but no further action was required as all remaining users still required "Web-admin" rights.
- Customer Impact: None
- Root Cause Analysis: In previous years this has not been an issue as there was only a single Interxion AD group synching with Azure AD. Because of the OneDigital migration project this was out of sync with some on-prem Interxion AD groups in Azure showing users duplicated because of

the existence of two domains (Interxion.com and Digitalrealty.com). We were unaware of this fact when the review was performed.

- Corrective Action: All future reviews will take into consideration both AD and Azure users list until legacy Interxion stack is mothballed in 2023.
    - Status: Resolved

- Scope: IT EMEA
- Containment: Isolated the synchronisation between HRIS and AD and manual check on consistency.
- Customer Impact: None
- Root Cause Analysis: Due to restructuring identity registration received over time was incomplete and not discovered whilst automated import.
- Corrective Action:
    - Status: Resolved
    - Combined HR / IT correction activities executed; automation is corrected with additional check and re-activated.
    - JML process to be further extended to overcome scripting dependencies and detection of field changes. Project initiated.

5.2.8. Management response on deviation related to CC6.3 - control A:

- Scope: Local
- Containment: The AD user registration / de-registration process ensures that only active DLR users are granted access to the suite of applications. AD user registrations shall be reviewed quarterly for all local applications.
- Customer Impact: None
- Root Cause Analysis: Human error
- Corrective Action: None required
    - Status: Resolved

5.2.9. Management response on deviation related to CC6.4 - control A:

- Scope: Local
- Containment: User access groups have been split to allow a more granular access rights assignment.
- Customer Impact: None
- Root Cause Analysis: Existing access groups were not detailed enough.
- Corrective Action: With the implementation of the new DLR Group Access System (AMAG) access rights will be granted on individual access reader level.
    - Status: Resolved

5.2.10. Management response on deviation related to CC6.4 - control C:

- Scope: Local
- Containment: User access groups have been split to allow a more granular access rights assignment.
- Customer Impact: None
- Root Cause Analysis: Existing access groups were not detailed enough.
- Corrective Action: With the implementation of the new DLR Group Access System (AMAG) access rights will be granted on individual access reader level.
    - Status: Resolved

5.2.11. Management response on deviation related to CC7.1 - control A:

- Scope: IT EMEA
- Customer Impact: None
- Root Cause Analysis: With transferal of TVM responsibility to other department, organization of process and follow up activities and registration have changed causing gap in visibility on follow up of process.
- Corrective Action:
    - Status: In progress
    - Process is active, follow up on identified issues is present. Action in progress to implement a more consistent registration of planned and performed actions.

5.2.12. Management response on deviation related to CC7.2 - control B:

- Scope: IT EMEA
- Containment: None
- Customer Impact: None
- Root Cause Analysis: Whilst transferring the logging / monitoring to our SIEM solution, the existing logging was not kept active, leading to gap in time of available logging. Existing Process was not changed or affected in any way and continuous operational.
- Corrective Action:
    - Status: In progress
    - Process is active, follow up on identified issues is present. Action in progress to implement a more consistent registration of planned and performed action.

digitalrealty.com