A-LIGN

# BMC Software, Inc.

# Type 2 SOC 2 with Cloud Computing Compliance Controls Catalogue (C5) and ISAE 3000

2024

bmc

# REPORT ON BMC SOFTWARE, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY WITH C5 CRITERIA

**Pursuant to Reporting on System and Organization Controls 2 (SOC 2)**
**Type 2 examination performed under AT-C 105 and AT-C 205 and ISAE 3000**

**January 1, 2024 to December 31, 2024**

# Table of Contents

# SECTION 1

# ASSERTION OF BMC SOFTWARE, INC. MANAGEMENT

## ASSERTION OF BMC SOFTWARE, INC. MANAGEMENT

November 22, 2024

We have prepared the accompanying description of BMC Software, Inc.'s ('BMC' or 'the Company') Helix Cloud Subscription Services System titled "BMC Software, Inc.'s Description of Its Helix Cloud Subscription Services System throughout the period January 1, 2024 to December 31, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Helix Cloud Subscription Services System that may be useful when assessing the risks arising from interactions with BMC Software, Inc.'s system, particularly information about system controls that BMC Software, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the criteria set forth in the Cloud Computing Compliance Controls Catalogue (C5 Criteria).

BMC Software, Inc. uses Amazon Web Services ('AWS'), Microsoft Azure ('Azure'), Google Cloud Platform ('GCP'), Equinix, Inc. ('Equinix'), and Oracle, Inc. ('Oracle') to provide data hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BMC Software, Inc., to achieve BMC Software, Inc.'s service commitments and system requirements based on the applicable trust services criteria and C5 criteria. The description presents BMC Software, Inc.'s controls, the applicable trust services criteria, C5 criteria, and the types of complementary subservice organization controls assumed in the design of BMC Software, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BMC Software, Inc., to achieve BMC Software, Inc.'s service commitments and system requirements based on the applicable trust services criteria and C5 criteria. The description presents BMC Software, Inc.'s controls, the applicable trust services criteria, C5 criteria, and the complementary user entity controls assumed in the design of BMC Software, Inc.'s controls.

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

a. the description presents BMC Software, Inc.'s Helix Cloud Subscription Services System that was designed and implemented throughout the period January 1, 2024 to December 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that BMC Software, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and C5 criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of BMC Software, Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that BMC Software, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria and C5 criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of BMC Software, Inc.'s controls operated effectively throughout that period.

Keith Corell
AVP - Procurement
BMC Software, Inc.

# SECTION 2

# INDEPENDENT SERVICE AUDITOR'S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To: BMC Software, Inc.

*Scope*

We have examined BMC Software, Inc. accompanying description of its Helix Cloud Subscription Services System titled "BMC Software, Inc.'s Description of Its Helix Cloud Subscription Services System throughout the period January 1, 2024 to December 31, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that BMC Software, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Cloud Computing Compliance Controls Catalogue (C5 Criteria).

BMC Software, Inc. uses AWS, Azure, GCP, Equinix, and Oracle to provide data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BMC Software, Inc., to achieve BMC Software, Inc.'s service commitments and system requirements based on the applicable trust services criteria and C5 criteria. The description presents BMC Software, Inc.'s controls, the applicable trust services criteria, C5 criteria, and the types of complementary subservice organization controls assumed in the design of BMC Software, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BMC Software, Inc., to achieve BMC Software, Inc.'s service commitments and system requirements based on the applicable trust services criteria and C5 criteria. The description presents BMC Software, Inc.'s controls, the applicable trust services criteria, C5 criteria, and the complementary user entity controls assumed in the design of BMC Software, Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

*Service Organization's Responsibilities*

BMC Software, Inc. 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 BMC Software, Inc.'s service commitments and system requirements were achieved. BMC Software, Inc. has provided the accompanying assertion titled "Assertion of BMC Software, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. BMC Software, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and C5 criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard of Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and C5 criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- 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 and C5 criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and C5 criteria
- Evaluating the overall presentation of the description

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

*Independence and Ethical Responsibilities*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

*Service Auditor's Independence and Quality Control*

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

*Inherent Limitations*

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls 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 and C5 criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

*Description of Tests of Controls*

The specific controls we tested and the nature, timing, and results of those tests are listed in section 4.

*Opinion*

In our opinion, in all material respects,

a. the description presents BMC Software, Inc.'s Helix Cloud Subscription Services System that was designed and implemented throughout the period January 1, 2024 to December 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that BMC Software, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and C5 criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of BMC Software, Inc.'s controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that BMC Software, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria and C5 criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of BMC Software, Inc.'s controls operated effectively throughout that period.

*Restricted Use*

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of BMC Software, Inc., user entities of BMC Software, Inc.'s Helix Cloud Subscription Services System during some or all of the period January 1, 2024 to December 31, 2024, business partners of BMC Software, Inc. subject to risks arising from interactions with the Helix Cloud Subscription Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria and C5 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.


Tampa, Florida
January 18, 2024

# SECTION 3

# BMC SOFTWARE, INC.'S DESCRIPTION OF ITS HELIX CLOUD SUBSCRIPTION SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2024 TO DECEMBER 31, 2024

## OVERVIEW OF OPERATIONS

### Company Background

In an era of constant change, the ability to adapt quickly and turn challenges into opportunities is critical. BMC helps companies around the world run and reinvent their businesses to evolve to an Autonomous Digital Enterprise, a digital-first organization with distinct tech tenets and operating model characteristics that support transformation through actionable insights, business agility, and customer centricity. The BMC portfolio comprises durable and daring technology along with comprehensive and highly effective services, dedicated to empowering today's businesses with intuitive, scalable solutions for intelligent automation and service management, enterprise DevOps, mainframe modernization, IT optimization, security and compliance, and so much more, from your multi-cloud infrastructure to your core data center and beyond.

Established in 1980, originally founded to help companies optimize their investment in mainframe technology, in the past 44 years, BMC has expanded the expertise through organic growth, strategic acquisitions, and relentless research and development to include infrastructure, networks, and services in distributed environments across the data center and into multi-cloud. Throughout the journey, BMC has been dedicated to enabling innovation and increasing visibility, security, and availability across Information Technology (IT) infrastructure and services.

BMC's core values guide the company's culture and customer relationships, driving business decisions and corporate direction. BMC's dedication to customer success is reflected in thriving global community, made up of tens of thousands of IT professionals, representing six continents and 131 countries. BMC welcomes over one million visitors to the BMC Community, where customers learn and share their knowledge as they discuss technology trends and the latest updates about BMC products and solutions. As part of the dedication to the communities BMC engages in worldwide, BMC encourages and promote employee participation through BMC Cares, global corporate social responsibility (CSR) program that empowers the workforce with curated in-person and virtual volunteer opportunities that support digital literacy, interventions, and accessibility. BMC is a member of the united nations (UN) Global Compact, and diversity, equity, and inclusion (DEI); environmental, social, and governmental (ESG); and CSR initiatives are guided by the United Nations Sustainable Development Goals (SDGs), a universal call intended to end poverty, protect the planet, and ensure people enjoy peace and prosperity.

As businesses embark on the journey to an Autonomous Digital Enterprise, the opportunities presented by expanding platforms, development models, technologies, and data sets are met with corresponding challenges.

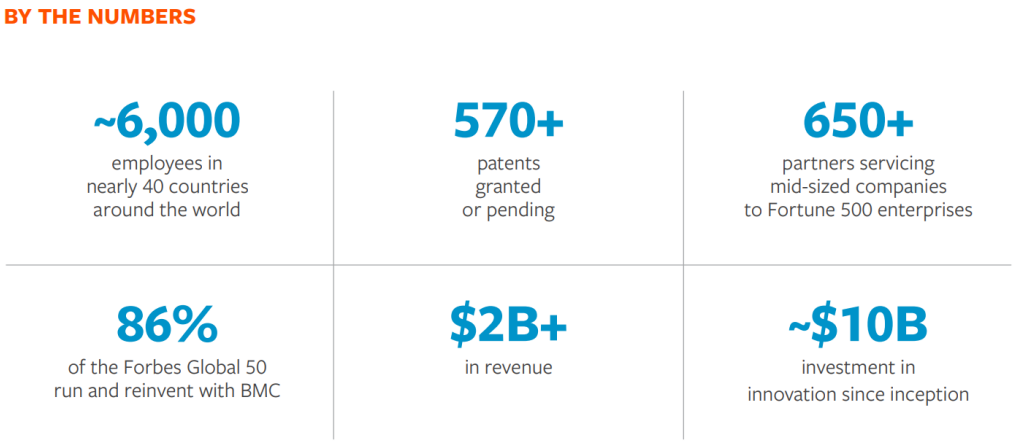
The comprehensive BMC IT management portfolio helps companies in every industry harness opportunity and deliver value with competitive differentiation enabled by actionable insights, business agility, and customer centricity. From artificial intelligence for IT operations (AIOps) to artificial intelligence service management (AISM) and from DevOps to DataOps, forward-looking solutions can empower your business to thrive in an era of constant change.

### Description of Services Provided

BMC provides Software as a Service (SaaS) solutions for businesses, helping companies around the world put technology at the forefront of business transformation by improving the delivery and consumption of digital services. Key company tenets include:

- Founded in September 1980
- Privately held
- More than 15,000 customers in more than 120 countries
- Technical alliances and partnerships with over 650+ companies worldwide

- Patents for technological innovation: 570+ pending or granted




**Principal Service Commitments and System Requirements**

BMC designs its processes and procedures related to BMC Helix Cloud Subscription Services System to meet the objectives based on the service commitments that it makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that it has established for the services. The BMC Helix Cloud Subscription Services System are subject to the security and privacy requirements of its corporate policies in regard to security, availability, and confidentiality, as amended, including relevant regulations, as well as the applicable state privacy security laws and regulations in the jurisdictions in which it operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the BMC Helix Cloud Subscription Services System that are designed to permit system users to access only the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and over untrusted networks

BMC establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in BMC's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the BMC Helix Cloud Subscription Services System.

**Components of the System**

*Infrastructure*

The primary infrastructure used to provide the BMC Helix Cloud Subscription Services System include the following:

| **Primary Infrastructure** | | |
|---|---|---|
| **Hardware** | **Type** | **Purpose** |
| Serial Console Server | Server | Serial Console Server for centralized, secure remote data center and out-of-band management of IT assets and Internet of Things (IoT) devices |
| Network Firewall | Firewall | Firewalls for a context-aware, network-centric approach to security that enables consistent security enforcement |
| Application Delivery Controller (ADC) | Controller | ADC provides total visibility, flexibility, and control across application delivery services |
| Local Traffic Manager (LTM) | Traffic Manager | LTM for Application Delivery Networks acts as a full proxy between users and application servers, providing a layer of abstraction that secures, optimizes, and load balances application traffic |
| Router | Router | Integrated services routers offering offers secure Wireless Area Network (WAN) connectivity, application experience, unified communications, network automation, virtualization, and branch and direct Internet access security solutions in one platform |
| Fabric Extender | Fabric Extender | Fabric Extender with greater port density and a lower oversubscription rate that supports massively scalable 1 and 10 Gigabit Ethernet environments with fewer management points using the fabric extender architecture and enables transparent migration to 10 Gigabit Ethernet, virtual machine-aware unified fabric technologies |
| Switch | Switch | Switch optimized for scalability, high performance, investment protection, and flexibility for traditional, virtualized, and cloud environments |
| Application Firewall | Firewall | Next-generation firewall that can be deployed in a range of private and public cloud computing environments |
| Switch | Switch | Enterprise-class stackable Gigabit Ethernet Layer 2 and Layer 3 access switches |

*Software*

Primary software used to provide the BMC Helix Cloud Subscription Services System includes the following:

| **Primary Software** | |
|---|---|
| **Software** | **Purpose** |
| BMC Helix ITSM | Provides out-of-the-box-oriented IT Service Management functionality for the following processes (limited based on the package purchased): incident, problem, change, release, asset, service level management, service request management, and knowledge management, and configuration management. Includes components such as AR System platform, Configuration Management Database (CMDB), Smart Reporting, Information Technology Service Management (ITSM) Applications, and Smart IT UI. BMC Helix can be licensed via 3 different packaging options:<br>• BMC Helix ITSM Service Desk<br>• BMC Helix ITSM Service Optimization<br>• BMC Helix ITSM Suite |
| BMC Helix Digital Workplace Basic | A next-generation, self-service application for business users to connect with IT and Human Resource (HR) anywhere, any time, on any device. The Basic subscription includes assistance, approvals, and general broadcasts |
| BMC Helix Digital Workplace Advanced | Extends the Basic subscription to include Follow capabilities and Location and Service Health features, as well as the Virtual Chat and Digital Workplace Catalog |
| BMC Helix Client Management service | BMC Client Management provides an accurate view of software installations, ensures device adherence to organizational and industry policies, and supports systems and software currency |
| BMC Helix Business Workflows | BMC Helix Business Workflows is a modern case management solution that extends services for lines of business including HR, Facilities, and other groups. This solution allows users to create and automate workflows using pre-defined functionality and leverages cognitive capabilities to eliminate manual work |
| BMC Helix Cognitive Automation and Cognitive Search Service | Transform from ITSM to Cognitive Service Management by adding the BMC Helix Cognitive Automation service. Using IBM Watson machine learning and conversation capabilities, this service enables you to automate your application workflow tasks, such as assignment and categorization |
| BMC Helix Premium Connector service | This service allows you to easily design and automate event-driven tasks across applications by using out-of-the-box connectors or developing your own |
| BMC Helix Discovery | BMC Helix Discovery is a cloud-native discovery and dependency mapping solution that provides visibility into hardware, software, and service dependencies across your environments |
| BMC Helix Communications Service Providers Service | BMC Helix for CSP (Communication Service Providers) customers with information specific to service operations |
| BMC Helix Innovation Suite Service | BMC Helix Innovation Studio (formerly known as BMC Helix Platform) is a part of the single-tenant BMC Helix Innovation Suite that consolidates the capabilities of Action Request System and BMC Helix Innovation Studio |

| Primary Software | |
|---|---|
| **Software** | **Purpose** |
| BMC Helix Cloud Cost Service | BMC Helix Cloud Cost Service is a cloud-based digital platform that tracks cost utilization and expenditure by collecting, organizing, and analyzing high volumes of volatile IT business data, in real time, to meet the demands of web-scale IT. Complete and accurate analysis empower IT operations to make fast, data-driven decisions that support continuous digital service improvement and innovation |
| BMC Helix Cloud Security Service | BMC Helix Cloud Security is a cloud-based digital platform that tracks regulatory and security compliance by collecting, organizing, and analyzing high volumes of volatile IT business data |
| BMC Helix Innovation Studio - Reporting User Service | BMC Helix Platform is a combination of services and components that helps you develop, build, deploy, and use multi-tenant applications on cloud. It also helps you to create and automate many business processes without learning a programming language or complex development tools |
| BMC Helix and Innovation Studio Services | BMC Helix Platform is a combination of services and components that helps you develop, build, deploy, and use multi-tenant applications on cloud. It also helps you to create and automate many business processes without learning a programming language or complex development tools |
| BMC Helix Automation Console | BMC Helix Automation integrates with TrueSight Server Automation to identify, analyze, and remediate missing patches, vulnerabilities, and compliance violations in your environment |
| BMC Helix Continuous Optimization | BMC Helix Continuous Optimization is a cloud-based capacity management solution that gives you insights to optimize the use of your current IT resources and plan for future demands. It collects and analyzes the capacity data and core metrics for central processing unit (CPU), memory, and storage, and provides recommendations for optimizing them |
| BMC Helix Client Management Service | BMC Client Management automates client management helping organizations control costs, maintain compliance, and reduce data and financial risks |
| BMC Helix Intelligent Automation Service | BMC Helix Intelligent Automation is an automation aggregator that enables organizations to connect with automation tools of their choice and define policies to trigger remediation actions |
| BMC Helix IT Operations Management (ITOM) Bundles Services (Standard and Advanced) | BMC Helix ITOM Standard provides core IT operations capabilities to discover, monitor, and optimize your traditional and multi-cloud resources.<br>BMC Helix ITOM Advanced provides the core IT operations capabilities in the Standard licensing, plus advanced use cases for comprehensive resource planning, business driver predications, publishing service models to the configuration management database (CMDB) and advanced reporting |
| BMC Helix iPaaS Service | BMC Helix iPaaS is an integration solution that offers connectors and out-of-the box integrations to address advanced business process and system integration challenges for digital enterprises |
| BMC Helix ITSM Service Desk service | BMC Helix ITSM Service Desk provides the following environments:<br>• Development<br>• Quality Assurance<br>• Production |

| Primary Software | |
|---|---|
| **Software** | **Purpose** |
| BMC Helix ITSM Service Optimization service | BMC Helix ITSM Service Optimization provides the following environments:<br>• Development<br>• Quality Assurance<br>• Production |
| BMC Helix ITSM Suite service | BMC Helix ITSM Suite provides the following environments:<br>• Development<br>• Quality Assurance<br>• Production |
| BMC Helix Knowledge Management by ComAround service | BMC Helix Knowledge Management by ComAround service is available as the following:<br>• BMC Helix Knowledge Management by ComAround standalone<br>• BMC Helix Knowledge Management by ComAround with BMC Helix Virtual Agent Advanced |
| BMC Helix Multi-Cloud Broker service | BMC Helix Multi-Cloud Broker is a ticket-brokering add-on service for BMC Helix ITSM with BMC Helix iPaaS powered by Jitterbit, or powered by MuleSoft, as the underlying technology |
| BMC Helix Operations Management service | BMC Helix Operations Management service and is monitoring and event management offering |
| BMC Helix Portfolio Management service | BMC Helix Portfolio Management provides the following environments:<br>• Tailoring<br>• Quality Assurance<br>• Production |
| Fusion Agility Suite and Visual Boards for BMC Helix (Version 21.3 and 20.08) | Fusion Agility Suite / Visual Boards for BMC Helix provides the following environments:<br>• Tailoring<br>• Quality Assurance<br>• Production |
| BMC Helix Virtual Agent Basic service | BMC Helix Virtual Agent Basic provides the following environments:<br>• Tailoring (BMC Helix Virtual Agent only)<br>• Quality Assurance (BMC Helix Virtual Agent only)<br>• Production (BMC Helix Virtual Agent and BMC Helix Knowledge Management by ComAround) |
| BMC Helix Virtual Agent Advanced service | BMC Helix Virtual Agent Advanced provides the following environments:<br>• Tailoring (BMC Helix Virtual Agent only)<br>• Quality Assurance (BMC Helix Virtual Agent only)<br>• Production (BMC Helix Virtual Agent and BMC Helix Knowledge Management by ComAround) |
| Catchpoint for BMC Helix | Catchpoint's Internet Performance Monitoring (IPM) suite offers synthetics, RUM, performance optimization, high fidelity data and flexible visualizations with advanced analytics |
| Digital.ai for BMC Helix | Digital.ai Change Risk Prediction and Management Process Optimization |

| Primary Software | |
|---|---|
| **Software** | **Purpose** |
| BMC Helix AIOps and observability service | BMC Helix AIOps and Observability - Standard provides core IT operations capabilities to discover, monitor, and optimize your traditional and multi-cloud resources |
| BMC Helix Platform service | BMC Helix Platform is a combination of services and components that helps you develop, build, deploy, and use multi-tenant applications on cloud. It also helps you to create and automate many business processes without learning a programming language or complex development tools |
| BMC Helix Integration Service | With BMC Helix Integration Service, you can easily design and automate event-driven tasks across applications |
| BMC Helix Network Service Operations for Communication Service Providers | With BMC Helix Network Service Operations for Communication Service Providers, BMC extends the Helix IT Service Management excellence into the CSP's (Communications Service Provider) Network Operations Center (NOC) |
| BMC Helix Customer Service Management service | BMC Helix Customer Service Management enables organizations to ease multiple challenges and provides business advantage |
| BMC Helix Service Management service | BMC Helix Service Management is a simplified packaging and pricing model for a suite of service management products, including BMC Helix ITSM, BMC Helix Digital Workplace, Lines of Business, and other services |
| BMC Helix Dashboards Service | BMC Helix Dashboards offers unified reporting and gives you a consolidated view of data from applications across your environment. The consolidated view of dashboards helps you perform tasks such as responding to issues quickly so that system downtime is minimized. You can create, export, and share interactive and customizable dashboards with users within or outside your environment. You can also improve the efficiency of your system by monitoring the key performance metrics |

*People*

BMC's SaaS Operations team is comprised of multiple roles to support sales, operations, support, security, governance, and customer success management. A brief summary of each role is as follows:

- Business Operations - This team manages business development activities in support of the global BMC sales organization. Duties include participation in customer briefings, pre-sales support, request for proposal (RFP) responses, and management of external documentation. Additionally, this team is responsible for finance, order management and backend operations.
- BMC SaaS Operations - This team supports technical operations for BMC's data center locations worldwide. The team is comprised of application, database, automation, capacity management, network, and infrastructure specialists who hold a variety of technical and professional certifications. Application owners manage system activation as well as upgrades for customers for each application.
- BMC SaaS Service Desk - This team manages support requests for BMC Helix customers. Responsibilities include general issue triage, application management, patch and release management, problem management, change management and work order fulfillment. This team is located in the U.S., U.K., Mexico, and India and follows a 24x7 support model.
- BMC Information Security - BMC's Helix Information Systems Security Officer, along with other security personnel, are responsible for security strategy, planning, execution, and governance for security in support of commercial, public sector and U.S. FedRAMP programs. Their scope includes

physical security, network security and application security. The team manages and maintains BMC's Security Information and Event Management system and collaborates with the BMC Governance team on security-related certifications and audits.

- BMC Governance - This team is responsible for creating and maintaining BMC operational policies and for leading project management activities.
- BMC Customer Success - Located worldwide, this team helps provide a personalized experience for service delivery, including facilitating service review meetings and coordinating application upgrade projects. The team acts as the liaison between the customer and the BMC SaaS Operations staff for escalations, service delivery and overall service quality.

*Data*

Data management covers the policies, practices, and procedures for the administration of data usage in a BMC service, including how data is defined, processed, and protected.

Application data is generally defined as:

- Foundational data - People records (name, e-mail, user id), companies, organizations, product categorizations, etc.
- Process data - Customer-defined templates, application workflow, etc.
- Transactional data - Customer-input incidents, work orders and change requests, and related structures.

The type of data input into foundational and transactional records is the customer's choice. BMC has no control over these inputs. Some process data is provided out-of-the box but may be modified and/or augmented by the customer. The ongoing configuration and modification of these types of data structures are fully managed by the customer. Customers retain ownership of their data at all times. BMC acts as the processor of data via its systems. Data is processed and stored within the same country where the system is located. Data is stored within a database dedicated to each customer and no data is co-mingled.

Data in transit is encrypted via Hyper Text Transfer Protocol Secure (HTTPS). Data at rest is encrypted via Advanced Encryption Standard (AES) 256 minimum. Character field-level encryption is also available if required.

Archiving data is an essential step in data management. It provides a way to remove obsolete records from the production database using a regular, controlled, and predictable process. Archiving data also helps to maintain system performance and to comply with record retention policies. Individual customer business needs dictate retention and archival requirements.

Upon service termination, data is exported and returned to the customer. BMC then permanently removes the customer's data by destroying the database encryption keys and overwriting the data with binary zeroes.

*Processes, Policies and Procedures*

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Every team is expected to adhere to the BMC policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any BMC team member.

Managed by a governance board, BMC's policies and procedures cover ongoing operations necessary to ensure the security and reliability of systems residing in the data centers.

Policies are reviewed at least annually with signoff from the appropriate executive sponsors. Project management activities are ongoing, with the project portfolio consisting of routine maintenance activities to service-specific development projects.

The BMC Helix Cloud Subscription Services System is designed based upon NIST (National Institute of Standards and Technology) controls and standards to provide enterprise grade security for its customers. BMC utilizes a defense in depth methodology that focuses on redundant controls to prevent and mitigate impacts to the confidentiality, availability, and integrity of customer data and services.

Security event preparedness and response events are as described in the BMC incident response plan. A security incident, or offense, is defined as an event generated by an enterprise Security Information and Event Management (SIEM) system based on correlating logs and events from incoming log sources. The SIEM provides real-time analysis of security alerts generated by both user activity and data center components.

Change management is a critical part of ongoing operations and provides discipline and quality control to system maintenance activities. Whether a change is instigated by BMC or a customer, approvals are managed by a BMC advisory board who promotes communication and collaboration regarding the change and ensures that the impact of the change is minimized. Change requests are submitted via the customer portal and are usually executed within one day.

In order for customers to keep current on application releases, BMC makes application upgrades available one to two times per year. Upgrades are performed by the BMC SaaS Operations team based on a schedule mutually agreed to with each customer. Project planning, test planning and release strategy are part of the upgrade project and require participation from the customer for validation and acceptance testing.

Physical Security

BMC's service locations are at hosted co-location facilities with the following minimum specifications for physical security:

- All sites are manned 24x7x365, including delivery and shipping areas. Delivery and shipping areas are physically walled off from the co-location areas. Access is allowed by escort only, with biometric scanning required for visitors. Only BMC employees have access to the BMC locked cage within the data center
- Security fencing includes reinforced concrete, electric fencing, vapor barriers and bullet-resistant front doors. Alarm systems include alarm contacts, glass breakage detectors, motion detectors and tamper switches
- Closed caption TVs (CCTV) constantly monitor building and gate activity with CCTV feeds digitized and maintained onsite for 30 days. The CCTV feeds are archived for one year

BMC co-location vendors maintain physical and environmental security controls to prevent physical attacks and/or loss of availability. Each service location's physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. BMC monitors these controls by obtaining and reviewing the data center providers' SOC 2 report (or equivalent) of each co-location vendor on an annual basis.

All data centers have an automated building monitoring system that oversees facility power, environment, and backup systems. Refer to the "Subservice Organizations" section below for the controls in place around physical security.

Logical Access

BMC maintains a SaaS Access Control policy that is reviewed annually. This policy formally establishes access controls which include the entirety of BMC SaaS-related assets, people, processes, and services, and ensures that pertinent controls are in compliance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance requirements.

BMC's access controls to the data center infrastructure include authentication to the internal BMC SaaS network via virtual private network (VPN), plus authentication via BMC's Active Directory. Access protocol calls for least-privilege permissions controls, with password reset enforcement every six weeks. Initial access is requested via an online form, with review from BMC's Information Systems Security Officer prior to access grant. User access is logged and auditable.

Employee termination calls for user ID deletion within one business day; employee re-assignment (within BMC) calls for user ID deletion within 30 days.

Computer Operations - Backups

BMC performs daily, weekly, and monthly backups for all environments for both the virtual machines (VMs) and databases. Backup and restore procedures are tested at least annually. Backups are stored both at the primary and secondary site locations.

Computer Operations - Availability

System availability is dependent on many aspects of BMC internal operations including networking components, hardware infrastructure, application, and database. The risks that would prevent BMC from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

BMC has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient Internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

In evaluating the suitability of the design of availability controls, BMC considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of back-up procedures, the reliability of the back-up process, and the ability to restore backed-up data. In evaluating the design of data availability controls, BMC considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system elements.

BMC addresses vulnerabilities by assessing the probability and impact of a risk event. Proactive management of these potential events enables BMC to make well-informed risk management decisions. Risk management starts in the product development phase where products are designed and developed using stringent code, program, and data review practices to ensure delivery of a secure and reliable application. BMC follows Open Web Application Security Project (OWASP) standards to proactively detect security-related issues in the code and any third-party libraries in its solutions.

BMC provides redundant controls at all layers of the architecture stack, eliminating any single point of failure. BMC regularly validates its environmental control systems, data backup and recovery procedures, user access controls, and disaster recovery processes. Full disaster recovery tests are performed in each data center location at least annually.

Change Control

BMC's Change Management policy defines the scope for any system change initiated by BMC or a customer. Scope includes changes to the hardware infrastructure, operating system, network, system-level configurations, database, and application.

Changes are managed by a change advisory board that holds responsibility for change-related processes including implementation, back out and remediation, scheduling, and customer communications.

Customer-initiated changes are submitted via the support portal and require a detailed description of the change including purpose and expected outcome, implementation procedures, back out procedures, change impact and risk, prerequisites, and related documentation. Change implementation is available 24x7 and is scheduled based on customer release requirements.

Data Communications

BMC's perimeter security layer focuses on ensuring data in motion is encrypted, as well as ensuring that access into the environment is restricted to the minimum access required. Key features of this layer include:

- Tiered Internet-facing web applications
- Strict HTTPS compliance for all ports and protocols
- Industry-standard, fully redundant stateful firewalls
- Intrusion prevention system (IPS) proactively monitors and blocks malicious network traffic activity
- Security Assertion Markup Language (SAML) 2.0 single sign-on support
- HTTPS Transport Layer Security (TLS)
- Transport Layer Security (TLS) utilization ensures secure e-mail and data file transmissions
- Secure Socket Layer (SSL) certificates (2048-bit)
- Third-party perimeter, network and application penetration tests conducted at least annually

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by BMC. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on an least an annual basis in accordance with BMC's policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by BMC. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an annual basis. Scans are performed during non-peak windows. Tools requiring installation in the BMC system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

*Cloud Service Security Program Processes, Policies and Procedures*

BMC Software has developed a cloud service security management program to meet the information security and compliance requirements related to Helix Cloud Subscription Services System services and its customer base. The program incorporates the elements of the C5 criteria catalogue. The description below is a summary of general conditions that BMC Software has implemented to adhere to the applicable components of C5 criteria.

BC-01 Information on Jurisdiction and Locations

The Company provides its customers with comprehensible and transparent information on its jurisdiction and system component locations. The Company's jurisdiction is limited to the US and its system components are located within the southwest portion of the US.

BC-02 Information on Availability and Incident Handling During Regular Operation

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

The Company has established a minimum acceptable performance level and has documented the acceptable response times and recovery times for disruptions of regular operation. This information can be found in the service level agreements as well as the company's website.

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network and with respect to the cloud services rendered.

BC-03 Information on Recovery Parameters in Emergency Operation

The Company includes in its business continuity plan and service level agreements information on the following recovery parameters of its cloud services:

- Maximum tolerable downtime / Recovery Time Objective (RTO)
- Maximum allowable data loss / Recovery Point Objective (RPO)
- Recovery time to start emergency operation
- Recovery level (i.e., capacity)
- Restore time until normal operation

The Company performs a business continuity test annually as well as a business impact analysis annually.

BC-04 Information on the Availability of the Data Center

The Company has formally documented and defined the availability of the data center to ensure no disruptions to business operations in the event of a disaster. The includes documenting the data center's availability and downtown annually.

In the event that a primary data center fails, the redundant data center is configured to take its place.

BC-05 Information on How Investigation Inquiries from Government Authorities Are Handled

The Company has formally documented in its service level agreements and on the company website how investigation inquiries by government agencies are handled. This also includes:

- Formally documented procedures for its employees on how to verify and handle such legal inquiries
- Formally documented procedures for informing and involving cloud customers upon receipt of such inquiries
- How affected cloud customers can object; and
- Whether the Company has the ability to decrypt encrypted data of the cloud customers in case of such a request and how this ability for access or disclosure is used.

BC-06 Information on Certifications or Attestations

The Company has worked with independent auditors annually to obtain the following valid certifications and attestations:

- Type 2 SOC 2.
- ISO 27001.

### Boundaries of the System

The scope of this report includes the BMC Helix Cloud Subscription Services System included in the Virtual Office Environment facilities.

The scope of this report does not include the data hosting services provided by AWS, Azure, GCP, Equinix (referred to as BMC Cloud), and OCI at various locations.

## RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

### Control Environment

*Integrity and Ethical Values*

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of BMC's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of BMC's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks (where allowed per local law) are performed for employees as a component of the hiring process.

BMC enforces a Code of Conduct that addresses acceptable business practices, conflicts of interest and expected standards of ethical and moral behavior. This document is provided to new employees. Employees are required to sign an acknowledgement form that they received and agree to follow the employee manual and Code of Conduct. There is an established "tone at the top", including explicit guidance about what is right and wrong. This tone is communicated and practiced by executives and management throughout the organization. The importance of high ethics and controls is discussed with newly hired employees throughout both the interview process and orientation.

*Commitment to Competence*

BMC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Over 80% of BMC's support and application management resources are BMC certified on the BMC Helix ITSM platform. Additional certifications held by various resources include, but are not limited to:

- ITIL - Information Technology Infrastructure Library (including foundational skills and various specialty levels)
- PMP - Project Manager Professional
- CISSP / ISSAP - Certified Information Systems Security / Information Systems Security Architecture Professional
- MCSE + Security - Microsoft Certified Security Engineer + Security
- C/CISO - Certified Chief Information Security Officer
- NSA-IAM - National Security Agency InfoSec Assessment Methodology
- CEH - Certified Ethical Hacker
- CICRA - Certified Internal Controls Risk Analyst (ISO 27005)
- ACE - Palo Alto Accredited Configuration Engineer
- CCNA - Cisco Certified Network Associate
- CISA - Certified Information Systems Auditor
- ISO 27001 - Lead Implementor

Commitments are communicated in written individualized agreements, Service Level Agreements (SLAs), or published statements. Commitments are provided via written communication and may also come in the form of online documentation, published white papers or system broadcast messages. BMC's commitments include, but are not limited to, the following:

- Scope of services provided including application access, license capacity limits and usage rights
- Support services including incident classification and hours of coverage
- Service levels including system availability and warranties
- Published operational policies
- Security and data protection standards

*Management's Philosophy and Operating Style*

BMC's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

BMC senior leadership team takes a "hands on" approach to running the business. Senior management is heavily involved in every phase of the business operations.

BMC has at least one monthly staff meeting that enables the senior management team to remain in close contact with personnel and to consistently emphasize appropriate behavior to personnel and to key vendor personnel. This team demonstrates attitudes and actions that consistently reflect a commitment to delivering quality services, superior customer support, and ethical values.

*Organizational Structure and Assignment of Authority and Responsibility*

BMC's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

BMC's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

*Human Resources Policies and Practices*

BMC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. BMC's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

*Information Security Framework*

BMC Software follows a systematic approach for developing, implementing, and managing its information security program. This includes defining business objectives and the scope / boundaries of the in-scope systems, performing regular risk assessments to identify the critical assets and threats and mitigation strategies, leveraging an existing security framework (e.g., ISO 27001; NIST Cybersecurity Framework, COBIT, etc.), formalizing information security policies and procedures, implementing controls and regular security awareness training, monitoring the in-scope environment for anomalies, attacks and threats, and implementing a formal incident response plan to investigate and remediate identified issues.

*Periodic Assessments*

BMC Software has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by BMC Software to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the relevant personnel on an annual basis:

- *Risk Assessment*: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality.
- *Cloud Service Security Risks*: Cloud service security risks are assessed by the Chief Information Security Officer (CISO). Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CISO of the organization.

*Periodic Testing and Evaluation*

BMC Software completes evaluations throughout each calendar year regarding the effectiveness of the

cloud service security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

*Policies and Procedures*

Cloud service security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all BMC Software personnel. These policies and procedures define guidelines for the cloud service security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Cloud information security policy
- Data classification
- Business continuity
- Incident management
- Access control
- Physical security

These policies are reviewed and approved by management on at least an annual basis.

*Identify and Access Management / Privileged Users*

BMC Software uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

Access is provisioned using the least-privileged concept and privileged access is limited to those requiring such access for business purposes.

*Cryptography and Key Management*

BMC Software has implemented robust cryptographic and key management practices for effectively safeguarding sensitive data that includes:

- Formally assessing the needs and risks of protecting data annually;
- Designing and formalizing a cryptographic strategy;
- Formally documenting a key management policy that outlines procedures for key generation, distribution, storage, rotation, revocation and destruction;
- Securing key generation through the use of trusted sources of randomness and entropy;
- Using secure channels for key distribution;
- Employing secure storage mechanisms for key cryptographic keys;
- Implementing policies for regular key rotation to mitigate the risk of key compromise; and
- Implementing monitoring and auditing mechanisms to track key usage, detect anomalies and ensure compliance with key management policies.

*Portability and Interoperability*

BMC Software has implemented portability and interoperability practices that includes:

- Establishing standardized formats, protocols, and interfaces for data exchange and communication within the organization;
- Embracing open standards and technologies that facilitate portability and interoperability across the

organization systems;
- Developing well-designed and documented APIs that expose functionalities in a clear, consistent, and secure manner;
- Standardizing data formats and serialization techniques to ensure compatibility and ease of data exchange.
- Implementing a centralized IAM solution to manage user access and permissions; and
- Implementing data mapping and transformation capabilities to facilitate seamless conversion between data formats, schemas, and structures.

*Security Awareness Training*

BMC Software employees receive security awareness training as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in annual security awareness training.

*Incident Response*

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

The Company's incident response process includes:
1. Developing a formal incident response plan
2. Establishing an incident response team
3. Identifying critical assets and systems
4. Implementing preventive and detective controls
5. Establishing communication channels
6. Identifying incidents timely through the monitoring capabilities
7. Analyzing and prioritizing the severity and criticality of incidents
8. Performing forensic analysis to determine the root cause
9. Containing the impact of the incident
10. Mitigating and remediating the identified incident
11. Documenting the identified incident including the resolution of the incident

*Vendor Management*

BMC Software maintains a formal vendor management process including assessing its vendors at least annually. The process followed includes:
- Performing due diligence procedures on any prospective vendor;
- Formally defining and executing a several level agreement that defines service levels, KPIs, and roles and responsibilities;
- Issue escalation;
- Performing a vendor risk assessment at least annually; and

*Business Continuity Management*

The Company has documented a formal business continuity plan that is tested at least annually. The business continuity procedures in place includes:
- Identifying potential risks
- Performing a business impact analysis
- Establishing recovery objectives
- Identifying recovery strategies

- Establishing an emergency response team
- Performing regular training and drills
- Defining the backup and recovery procedures
- Implementing redundancy and failover measures
- Communication to affected internal and external stakeholders

*Remediation and Continuous Improvement*

Areas of non-compliance in BMC Software's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

*Contractual and Compliance Requirements*

The Company has established formal procedures regarding managing contractual and compliance requirements that includes:

- Identifying and documenting the requirements outlined in contracts and compliance standards;
- Formally reviewing the compliance against contractual and compliance standards at least annually; and
- Performing internal audits to verify appropriate controls are in place and operating effectively to comply with contractual and compliance requirements.

*Government Investigation Requests*

The Company has established formal procedures to address allegations of misconduct, violations of policies, or breaches of ethical standards. The procedures include:

- Establishing a centralized process for receiving governance investigation requests;
- Ensuring governance investigation requests include detailed information and are assigned an unique identifier;
- Assigning governance investigation requests to a support team for investigating and responding to;
- Communicating the governance investigation request to impacted stakeholders;
- Performing an analysis and reporting on the investigation; and
- Following up to ensure the appropriate corrective actions and remedial measures were taken.

*Security Configurations and Logging*

The Company has formally established securing configurations and logging requirements for the in-scope systems in their information security policies and configuration baseline standards. The securing configurations and logging requirements are based on industry best practices and security frameworks and cover operating systems, network devices, databases, and applications.

*Authentication and Authorization*

The Company's authentication procedures includes:

- User identification
- Multi-factor authentication (MFA)
- Single-sign on to key systems
- Identify verification

- Session Management

The Company's authorization procedures includes:

- Role-based access controls
- Access control lists
- Permission management (including approval from management for access to critical systems and resources)
- Formal access provisioning and de-provisioning
- Access audit logging and monitoring
- Access reviews annually

**Risk Assessment Process**

BMC's risk assessment process identifies and manages risks that could potentially affect BMC's ability to provide reliable services to user entities. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. BMC identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by BMC, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

BMC has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. BMC attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management. BMC identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. The risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

Appropriate levels of management are involved in the risk assessment process. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. BMC's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk.

BMC considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets or data and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

BMC identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which BMC operates. BMC considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

As part of the risk assessment process, BMC determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

*Integration with Risk Assessment*

The environment in which the system operates, the commitments, agreements, and responsibilities of BMC's Digital Enterprise Management services, as well as the nature of the components of the system result in risks that the criteria will not be met. BMC addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, BMC's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

**Information and Communications Systems**

Information and communication are an integral component of BMC's internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At BMC, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, entity-wide meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the entity-wide meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate BMC personnel via e-mail messages.

Specific information systems used to support the BMC Helix Cloud Subscription Services System are described in the Description of Services Provided section above.

BMC has implemented various methods of communication to ensure that employees understand their individual roles and responsibilities. These methods include training programs for educating employees on internal developments, industry trends, and organizational development activities.

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

BMC obtains or generates and uses relevant, quality information to support the functioning of internal control. BMC maintains data flow diagrams, flowcharts, narratives, and procedural documentation to allow easy identification of data sources, responsible personnel, and other relevant information. BMC has methods in place to help ensure information systems maintain and produce information that is timely, current, accurate, and complete.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. BMC's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

*On-Going Monitoring*

BMC's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in BMC's Helix's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of BMC's personnel.

*Reporting Deficiencies*

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Members of BMC SaaS Operations and corporate IT organizations regularly participate in security / risk-based workshops to assess the impact of emerging technologies. Additionally, they hold weekly team meetings to discuss current projects and any potential security concerns.

Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

BMC selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. BMC's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

BMC 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. Guidelines for reporting deficiencies have been developed and are provided to employees.

**Changes to the System Since the Last Review**

No significant changes have occurred to the services provided to user entities since the organization's last review.

**Incidents Since the Last Review**

No significant incidents have occurred to the services provided to user entities since the organization's last review.

**Trust Services Criteria and Control Domain Requirements Not Applicable to the System**

All Common/Security, Availability, and Confidentiality criteria were applicable to the BMC Helix Cloud Subscription Services System.

The following C5 Control Domain Basic Requirements are not applicable to the system:

| C5 Basic Requirements Not Applicable to the System | | |
|---|---|---|
| **Control Domain** | **Control ID** | **Reason** |
| Operations | OPS-03 | The entity's service model does not allow for cloud customers to allocate system resources |
| Identity and Access Management | IDM-07 | Cloud customer data is not directly accessible to the entity's employees |
| Procurement, Development, and Maintenance of Information Systems | DEV-02 | The entity does not utilize external developers/ contractors for change management, release, and testing |
| Application and Interface Security | PSS-11 | Cloud customers are not responsible for operating or managing virtual machines directly within the in-scope applications' API or management consoles |

**Subservice Organizations**

The scope of this report does not include the data hosting services provided by Amazon Web Services ('AWS'), Microsoft Azure ('Azure'), Google Cloud Platform ('GCP'), Equinix (referred to as BMC Cloud), and Oracle ('OCI').

*Subservice Description of Services*

BMC uses Amazon Web Services ('AWS'), Microsoft Azure ('Azure'), Google Cloud Platform ('GCP'), Equinix (referred to as BMC Cloud), and Oracle ('OCI') for data hosting services to support the hosting of the application, which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

*Complementary Subservice Organization Controls*

BMC's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for the Trust Services Criteria related to BMC's services to be solely achieved by BMC control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of BMC.

The following subservice organization controls should be implemented by Amazon Web Services ('AWS') to provide additional assurance that the Trust Services Criteria described within this report are met:

| Subservice Organization - AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | CC6.4, | Physical access to data centers is approved by an authorized individual. |

| Subservice Organization - AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security, Physical Security (PS) | PS-01, PS-03, PS-04, PS-05, PS-06, PS-07 | Physical access is revoked within 24 hours of the employee or vendor record being deactivated. |
| | | Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. |
| | | Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations. |
| | | Physical access points to server locations are managed by electronic access control devices. |
| Availability, Portability and Interoperability (PI) | A1.2, PI-03 | Amazon-owned data centers are protected by fire detection and suppression systems. |
| | | Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels. |
| | | Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers. |
| | | Amazon-owned data centers have generators to provide backup power in case of electrical failure. |
| | | Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. |
| | | AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. |
| | | Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics. |
| | | Incidents are logged within a ticketing system, assigned severity rating, and tracked to resolution. |
| | | Critical AWS system components are replicated across multiple Availability Zones and backups are maintained. |
| | | Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones. |

The following subservice organization controls should be implemented by Microsoft Azure to provide additional assurance that the Trust Services Criteria described within this report are met:

| Subservice Organization - Azure | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security, Physical Security (PS) | CC6.4, CC7.2, PS-01, PS-03, PS-04, PS-05, PS-06, PS-07 | Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. |
| | | Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. |
| | | Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. |
| | | Physical access mechanisms (e.g., access card readers, biometric devices, man traps/portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. |
| | | The datacenter facility is monitored 24x7 by security personnel. |
| Availability, Portability and Interoperability (PI) | A1.2, PI-03 | Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. |
| | | Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems. |
| | | Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. |
| | | Backups of key Microsoft Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. |
| | | Critical Microsoft Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. |
| | | Customer data is automatically replicated within Microsoft Azure to minimize isolated faults. |
| | | Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. |
| | | Smoke detection devices are installed in all data centers. |
| | | Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities. |

| Subservice Organization - Azure | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Offsite backups are tracked and managed to maintain accuracy of the inventory information. |
| | | Production data is encrypted on backup media. |
| | | Microsoft Azure services are configured to automatically restore customer services upon detection of hardware and system failures. |

The following subservice organization controls should be implemented by GCP to provide additional assurance that the Trust Services Criteria described within this report are met:

| Subservice Organization - GCP | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security, Physical Security (PS) | CC6.4, PS-01, PS-03, PS-04, PS-05, PS-06, PS-07 | Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas. |
| | | Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks. |
| | | Data center perimeters are defined and secured via physical barriers. |
| | | Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner. |
| | | Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit. |
| | | Security measures utilized in data centers are assessed annually and the results are reviewed by executive management. |
| | | Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems. |
| Availability, Portability and Interoperability (PI) | A1.2, PI-03 | Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. |
| | | Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems. |

| Subservice Organization - GCP | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. |
| | | Backups of key GCP service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. |
| | | Critical GCP components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. |
| | | Customer data is automatically replicated within GCP to minimize isolated faults. |
| | | Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. |
| | | Smoke detection devices are installed in all data centers. |
| | | Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities. |
| | | Offsite backups are tracked and managed to maintain accuracy of the inventory information. |
| | | Production data is encrypted on backup media. |
| | | GCP services are configured to automatically restore customer services upon detection of hardware and system failures. |

The following subservice organization controls should be implemented by Equinix to provide additional assurance that the Trust Services Criteria described within this report are met:

| Subservice Organization - Equinix (Referred to as BMC Cloud) | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security, Physical Security (PS) | CC6.4, PS-01, PS-03, PS-04, PS-05, PS-06, PS-07 | Documented physical security standard operating procedures (SOPs) approved by management exist to provide guidance on restricting and controlling access to the data center facilities. |
| | | Procedures exist and are followed to establish and make changes to physical access privileges for employees. |
| | | Procedures exist and are followed to established and make changes to physical access privileges for customers. |

| Subservice Organization - Equinix (Referred to as BMC Cloud) | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Security personnel review a government issues ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to the facility. |
| | | Visitors are required to sign a visitor log upon entering facility. |
| | | Visitors are required to be escorted by an authorized employee when accessing the facility. |
| | | For the legacy facilities that employ onsite security, security personnel undergo a formal training program and their KPIs are reported and reviewed monthly. |
| | | A proximity card system and / or a biometric reader and personal identification number (PIN) are required to restrict access to the facility. |
| | | Physical access system logs are recorded and maintained for a minimum of six months. |
| | | Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras. |
| | | Surveillance camera logs are recorded and maintained for a minimum of 30 days. |
| | | Each customer has a defined space within the data center that is physically secured within a locked cage and / or cabinet. |
| | | Customers are required to sign a contract and nondisclosure agreement with Equinix. |
| | | The data center floor does not have any windows leading to the exterior of the building. In case due to the existing infrastructure there are windows leading to the exterior then they need to be locked form the inside or access controlled. |
| Availability, Portability and Interoperability (PI) | A1.2, PI-03 | Documented environmental security SOPs have been approved by management and are in place to help ensure that facilities have a consistent level of facility and environmental protection. |
| | | Each facility has been inspected by a local government official to ensure building code requirements have been met. |
| | | Each facility is monitored 24x7by onsite or on call facilities engineers. |
| | | Critical facility equipment is monitored 24x7 with alerts assigned to personnel to resolve any potential issue. |
| | | Power management equipment is in place for each facility. |
| | | Scheduled maintenance procedures are performed to test and confirm the operation of the power management system. |
| | | Fire detection and suppression equipment is in place at each facility. |

| Subservice Organization - Equinix (Referred to as BMC Cloud) | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly. |
| | | Air conditioning and ventilation equipment is in place at each facility to ensure that humidity levels and the required temperature are maintained. |
| | | Scheduled maintenance procedures are performed to ensure that the HVAC equipment and temperature and water detection sensors are working properly. |
| | | Insurance is in place for all locations and equipment. |
| | | Leak detection equipment is in place to help detect water presence where there should be none. |
| | | Emergency procedure documentation approved by management that addresses fires, bomb threats, severe weather, and medical emergencies is in place. |

The following subservice organization controls should be implemented by Oracle ('OCI') to provide additional assurance that the Trust Services Criteria described within this report are met:

| Subservice Organization - OCI | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security, Physical Security (PS) | CC6.4, CC7.2, PS-01, PS-03, PS-04, PS-05, PS-06, PS-07 | Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. |
| | | Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. |
| | | Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. |
| | | Physical access mechanisms (e.g., access card readers, biometric devices, man traps/portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. |
| | | The datacenter facility is monitored 24x7 by security personnel. |
| Availability, Portability and Interoperability (PI) | A1.2, PI-03 | Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. |
| | | Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems. |

| Subservice Organization - OCI | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. |
| | | Backups of key Oracle service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. |
| | | Critical Oracle components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. |
| | | Customer data is automatically replicated within Oracle to minimize isolated faults. |
| | | Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. |
| | | Smoke detection devices are installed in all data centers. |
| | | Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities. |
| | | Offsite backups are tracked and managed to maintain accuracy of the inventory information. |
| | | Production data is encrypted on backup media. |
| | | Oracle services are configured to automatically restore customer services upon detection of hardware and system failures. |

BMC management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, BMC performs monitoring of the subservice organizations controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding regular discussions with vendors and subservice organizations
- Making regular site visits to vendor and subservice organizations' facilities
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

**COMPLEMENTARY USER ENTITY CONTROLS**

BMC's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to BMC's services to be solely achieved by BMC control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of BMC.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to BMC.
2. User entities are responsible for notifying BMC of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of BMC services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize BMC services.
6. User entities are responsible for providing BMC with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying BMC of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

## TRUST SERVICES CATEGORIES

*In-Scope Trust Services Categories*

| **Common Criteria (to the Security, Availability, and Confidentiality Categories)** |
|---|
| Security refers to the protection of:<br>i. information during its collection or creation, use, processing, transmission, and storage; and<br>ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information. |

| **Availability** |
|---|
| Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance. |

| Confidentiality |
| --- |
| Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.<br><br>Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property. |

*Control Activities Specified by the Service Organization*

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of BMC's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at BMC are described within Section 4 and within the Subservice Organization Controls section above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

# SECTION 4

# TRUST SERVICES CATEGORY, CRITERIA, C5 CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

## GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, C5 CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of BMC was limited to the Trust Services Criteria and C5 criteria, related criteria and control activities specified by the management of BMC and did not encompass all aspects of BMC' operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205 and ISAE 3000.

Our examination of the control activities was performed using the following testing methods:

| TEST | DESCRIPTION |
|---|---|
| Inquiry | The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information. |
| Observation | The service auditor observed application of the control activities by client personnel. |
| Inspection | The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities. |
| Re-performance | The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control. |

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria
- Understand the aspects of the service organization's controls that may affect the C5 criteria
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria
- Determine whether the service organization's controls are suitably designed to achieve the C5 criteria

## CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC1.1 | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | Core values are communicated from executive management to personnel through policies, directives, guidelines, and the code of conduct. | Inspected the employee code of conduct, information security policies and procedures and the entity's shared drive to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, and the code of conduct. | No exceptions noted. |
| | | An employee code of conduct is documented to communicate workforce conduct standards and enforcement procedures. | Inspected the employee code of conduct to determine that an employee code of conduct was documented to communicate workforce conduct standards and enforcement procedures. | No exceptions noted. |
| | | Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. | Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct. | No exceptions noted. |
| | | Upon hire, personnel are required to complete a background check. | Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | Inquired of the Information Security Director regarding the annual performance review process to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | | Inspected the employee evaluation policy to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | | Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | Sanction policies which include termination is in place for employee misconduct. | Inspected the code of conduct to determine that sanction policies which include termination was in place for employee misconduct. | No exceptions noted. |
| | | An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. | Inspected the ethics hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC1.2 | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | Executive management roles and responsibilities are documented and reviewed annually. | Inspected the executive management job descriptions including revision dates to determine that executive management roles and responsibilities were documented and reviewed annually. | No exceptions noted. |
| | | Executive management maintains independence from those that operate the key controls within the environment. | Inspected the organizational chart and internal controls matrix to determine that executive management-maintained independence from those that operate the key controls within the environment. | No exceptions noted. |
| | | Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment. | Inspected the ISMS SaaS Management Review to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment. | No exceptions noted. |
| | | Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment. | Inquired of the Information Security Director regarding the risk register to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Observed the risk register to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment. | No exceptions noted. |
| | | | Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment. | No exceptions noted. |
| | | | Inspected the management's completed operational meeting discussion and risk management discussions to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment. | No exceptions noted. |
| CC1.3 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. | Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary. | Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary. | No exceptions noted. |
| | | Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. | Inspected the SaaS roles and responsibilities and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive. | No exceptions noted. |
| | | Executive management reviews job descriptions annually and makes updates, if necessary. | Inspected the revision history of the SaaS roles and responsibilities to determine that executive management reviewed job descriptions annually and made updates, if necessary. | No exceptions noted. |
| | | Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. | Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct. | No exceptions noted. |
| | | Executive management has established proper segregations of duties for key job functions and roles within the organization. | Inspected the organizational chart and SaaS roles and responsibilities to determine that executive management established proper segregations of duties for key job functions and roles within the organization. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system. | Inspected the SaaS roles and responsibilities to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system. | No exceptions noted. |
| CC1.4 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. | Inspected the internal employment policies and procedures and security awareness training policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel. | No exceptions noted. |
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | Inquired of the Information Security Director regarding the annual performance review process to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | | Inspected the employee evaluation policy to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | | Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process. | Inspected the human resources attestation for a sample of new hires and job descriptions to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process. | No exceptions noted. |
| | | The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. | Inspected the organizational chart to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives. | No exceptions noted. |
| | | Executive management has created a training program for its employees. | Inspected the information security and awareness training program to determine that executive management created a training program for its employees. | No exceptions noted. |
| | | Upon hire, personnel are required to complete a background check. | Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check. | No exceptions noted. |
| CC1.5 | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. | Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. | Inspected the SaaS roles and responsibilities and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive. | No exceptions noted. |
| | | Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. | Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct. | No exceptions noted. |
| | | Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. | Inspected the internal employment policies and procedures and security awareness training policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel. | No exceptions noted. |
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | Inquired of the Information Security Director regarding the annual performance review process to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | | Inspected the employee evaluation policy to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Environment** | | | | |
| **CC1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | Sanction policies which include termination is in place for employee misconduct. | Inspected the code of conduct to determine that sanction policies which include termination was in place for employee misconduct. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC2.1 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive. | Inspected the information security policies and procedures, the SaaS roles and responsibilities, and the entity's shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive. | No exceptions noted. |
| | | Edit checks are in place to prevent incomplete or incorrect data from being entered into the system. | Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system. | No exceptions noted. |
| | | Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system. | Inspected the data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system. | No exceptions noted. |
| | | Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access. | Inspected the encryption methods and configurations to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. | Inspected the SaaS roles and responsibilities and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive. | No exceptions noted. |
| | | The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's shared drive. | Inspected the entity's shared drive to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the entity's shared drive. | No exceptions noted. |
| | | Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | Inspected the signed employee handbook, code of conduct acknowledgement, and the completed information security and awareness training certificate for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the employee handbook and complete information security and awareness training. | No exceptions noted. |
| | | Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | Inquired of the Information Security Director regarding the training completion forms to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the information security and awareness training completion form for a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | No exceptions noted. |
| | | Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. | Inspected the signed code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct. | No exceptions noted. |
| | | Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities. | Inspected the ISMS Management Committee MoM and Action Plan to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities. | No exceptions noted. |
| | | An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. | Inspected the ethics hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's shared drive. | Inspected the incident response policies and procedures and the entity's shared drive to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's shared drive. | No exceptions noted. |
| | | The entity's objectives, including changes made to the objectives, are communicated to its personnel through the all-hands meeting. | Inspected the meetings notes for the all-hands meeting to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the all-hands meeting. | No exceptions noted. |
| CC2.3 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | The entity's third-party agreement delineates the boundaries of the system and describes relevant system components. | Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components. | No exceptions noted. |
| | | The entity's third-party agreement communicates the system commitments and requirements of third-parties. | Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties. | Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties. | No exceptions noted. |
| | | Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. | Inspected the agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements. | No exceptions noted. |
| | | Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers. | Inspected the BMC Cloud Services Master Agreement previous version history to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users, and customers. | No exceptions noted. |
| | | Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place. | Inspected the incident response policies and procedures and the helpline to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place. | No exceptions noted. |
| | | Executive management meets annually with operational management to discuss the results of assessments performed by third-parties. | Inspected the ISMS SaaS Management Review to determine that executive management met annually with operational management to discuss the results of assessments performed by third-parties. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Information and Communication** | | | | |
| **CC2.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. | Inspected the ethics hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. | No exceptions noted. |
| | | The entity communicates to external parties the system commitments and requirements relating to confidentiality through the use of third-party agreements. | Inspected the third-party agreement for a sample of third-parties to determine that the entity communicated to external parties, vendors, and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements. | No exceptions noted. |
| | | Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers. | Inspected the BMC Cloud Services Master Agreement previous version history to determine that changes to commitments and requirements relating to confidentiality were communicated to third-parties, external users, and customers. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC3.1 | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. | Inspected the organizational chart, internal employment policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics. | No exceptions noted. |
| | | Executive management has documented objectives that are specific, measurable, attainable, relevant, and time-bound ('SMART'). | Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART. | No exceptions noted. |
| | | Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. | Inquired of the Information Security Director regarding the risk register to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved. | No exceptions noted. |
| | | | Observed the risk register to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. | Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. | No exceptions noted. |
| | | Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities. | Inspected the SaaS roles and responsibilities, the organizational chart, and the risk management policies and procedures to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities. | No exceptions noted. |
| | | The entity has defined the desired level of performance and operation in order to achieve the established entity objectives. | Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. | Inspected the internal employment policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies. | No exceptions noted. |
| | | Business plans and budgets align with the entity's strategies and objectives. | Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives. | No exceptions noted. |
| | | Entity strategies, objectives and budgets are assessed on an annual basis. | Inspected the security budget and objective roadmap to determine that entity strategies, objectives and budgets were assessed on an annual basis. | No exceptions noted. |
| CC3.2 | COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | Documented policies and procedures are in place to guide personnel when performing a risk assessment. | Inspected the risk management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances. | Inspected the risk management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances. | No exceptions noted. |
| | | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inquired of the Information Security Director regarding the risk register to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |
| | | | Observed the risk register to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |
| | | | Inspected the internal risk audit to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The entity's risk assessment process includes:<br>• Identifying the relevant information assets that are critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks identified for each identified vulnerability | Inquired of the Information Security Director regarding the risk register to determine that the entity's risk assessment process included:<br>• Identifying the relevant information assets that were critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks identified for each identified vulnerability | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Observed the risk register to determine that the entity's risk assessment process included:<br>• Identifying the relevant information assets that were critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks identified for each identified vulnerability | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that the entity's risk assessment process included:<br>• Identifying the relevant information assets that were critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks identified for each identified vulnerability | No exceptions noted. |
| | | Identified risks are rated using a risk evaluation process and ratings are approved by management. | Inquired of the Information Security Director regarding the risk register to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Observed the risk register to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | Management develops risk mitigation strategies to address risks identified during the risk assessment process. | Inquired of the Information Security Director regarding the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |
| | | | Observed the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities. | Inquired of the Information Security Director regarding the risk register to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities. | No exceptions noted. |
| | | | Observed the risk register to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities. | No exceptions noted. |
| CC3.3 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | Management identifies and assesses the types of fraud that could impact their business and operations. | Inquired of the Information Security Director regarding the risk register to determine that management identified and assessed the types of fraud that could impact their business and operations. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Observed the risk register to determine that management identified and assessed the types of fraud that could impact their business and operations. | No exceptions noted. |
| | | | Inspected the internal risk audit to determine that management identified and assessed the types of fraud that could impact their business and operations. | No exceptions noted. |
| | | As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude. | Inquired of the Information Security Director regarding the risk register to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as opportunity for unauthorized access or use of data. | No exceptions noted. |
| | | | Observed the risk register to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as opportunity for unauthorized access or use of data. | No exceptions noted. |
| | | | Inspected the internal risk audit to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as opportunity for unauthorized access or use of data. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC3.4 | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. | Inquired of the Information Security Director regarding the risk register to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | | Observed the risk register to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. | Inquired of the Information Security Director regarding the risk register to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | | Observed the risk register to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Assessment** | | | | |
| **CC3.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment. | Inquired of the Information Security Director regarding the risk register to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | | Observed the risk register to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. | Inspected the ISPMS Management Review to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses. | No exceptions noted. |
| | | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |
| | | Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities. | Inspected the completed vulnerability scan for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities. | No exceptions noted. |
| | | A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment. | Inspected the completed penetration test results to determine that a penetration test was performed annually to identify and exploit vulnerabilities identified within the environment. | No exceptions noted. |
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | Inquired of the Information Security Director regarding the annual performance review process to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | | Inspected the employee evaluation policy to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis. | No exceptions noted. |
| | | Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | Inspected the completed third-party attestation reports including review for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | No exceptions noted. |
| | | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions 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. | Senior management assesses the results of the compliance, control and risk assessments performed on the environment. | Inspected the ISPMS Management Review to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Monitoring Activities** | | | | |
| **CC4.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions. | No exceptions noted. |
| | | Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were documented, investigated, and addressed. | No exceptions noted. |
| | | Vulnerabilities, deviations and control gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations and control gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions. | No exceptions noted. |
| | | Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner. | Inspected the audit issue tracker to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. | Inquired of the Information Security Director regarding the risk register to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. | No exceptions noted. |
| | | | Observed the risk register to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. | No exceptions noted. |
| | | | Inspected the supporting meeting notes for an example internal control that had failed to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. | Testing of the control activity disclosed that no incident ticket for an example internal control that had failed occurred during the review period. |
| | | Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. | Inspected the organizational chart and internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| Control Activities | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Management has documented the relevant controls in place for each key business or operational process. | Inspected the internal controls matrix to determine management documented the relevant controls in place for each key business or operational process. | No exceptions noted. |
| | | Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. | Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. | No exceptions noted. |
| | | Business continuity and contingency plans are developed and updated on an annual basis. | Inspected the business continuity and contingency plans to determine that business continuity and contingency plans were developed and updated on an annual basis. | No exceptions noted. |
| | | The business continuity plan is tested on an annual basis. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted. |
| CC5.2 | COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | Organizational and information security policies and procedures are documented and made available to employees through the entity's shared drive. | Inspected the information security policies and procedures and the entity's shared drive to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's shared drive. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. | Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. | No exceptions noted. |
| | | The internal controls implemented around the entity's technology infrastructure include, but are not limited to:<br>• Restricting access rights to authorized users<br>• Limiting services to what is required for business operations<br>• Authentication of access<br>• Protecting the entity's assets from external threats | Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to:<br>• Restricting access rights to authorized users<br>• Limiting services to what was required for business operations<br>• Authentication of access<br>• Protecting the entity's assets from external threats | No exceptions 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. | Organizational and information security policies and procedures are documented and made available to employees through the entity's shared drive. | Inspected the information security policies and procedures and the entity's shared drive to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's shared drive. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Control Activities** | | | | |
| **CC5.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel. | Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel. | No exceptions noted. |
| | | Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. | Inspected the SaaS roles and responsibilities and the entity's shared drive to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's shared drive. | No exceptions noted. |
| | | Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. | Inspected the internal controls matrix to determine performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. | Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring. | No exceptions noted. |
| | | An inventory of system assets and components is maintained to classify and manage the information assets. | Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets. | No exceptions noted. |
| | **Internal Network - Okta** | | | |
| | | Network user access is restricted via role-based security privileges defined within the access control system. | Inspected the network user listing and access roles to determine that network user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Network administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the network to determine that network administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the network administrator listing and access roles to determine that network administrative access was restricted to authorized personnel. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The network is configured to enforce password requirements that include:<br>• Password history<br>• Password age minimum<br>• Password age maximum<br>• Password length<br>• Complexity | Inspected the network password configurations to determine that the network was configured to enforce password requirements that included:<br>• Password history<br>• Password age minimum<br>• Password age maximum<br>• Password length<br>• Complexity | No exceptions noted. |
| | | Network and application users are authenticated via individually assigned user accounts and passwords. | Inquired of the Information Security Director regarding network authentication to determine that network users were authenticated via individually assigned user accounts and passwords. | No exceptions noted. |
| | | | Observed a user authenticate to the network to determine that network users were authenticated via individually assigned user accounts and passwords. | No exceptions noted. |
| | | Multi-factor authentication (MFA) is enabled and required to access the network. | Inspected the MFA configurations to determine that MFA was enabled and required to access the network. | No exceptions noted. |
| | | Network account lockout configurations are in place that include:<br>• Account lockout duration<br>• Account lockout threshold | Inspected the network account lockout configurations to determine that network account lockout configurations were in place that included:<br>• Account lockout duration<br>• Account lockout threshold | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Network audit logging configurations are in place that include user activity and system events. | Inspected the network audit logging configurations to determine that network audit logging configurations were in place that included user activity and system events. | No exceptions noted. |
| | | Network audit logs are maintained and available for review when needed. | Inquired of the Information Security Director regarding the network audit logs to determine that network audit logs were maintained and available for review when needed. | No exceptions noted. |
| | | | Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed. | No exceptions noted. |
| | **Operating Systems - Linux** | | | |
| | | Operating system user access is restricted via role-based security privileges defined within the access control system. | Inspected the operating system user listing and access roles to determine that operating system user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Operating system administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding the administrative access to the operating system to determine that operating system administrative access was restricted to authorized personnel. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the operating system administrator listing and access roles to determine that operating system administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Operating system users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that operating system users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |
| | | Operating system account lockout configurations are in place that include:<br>• Account lockout duration<br>• Account lockout threshold | Inspected the operating system account lockout configurations to determine that operating system account lockout configurations were in place that included:<br>• Account lockout duration<br>• Account lockout threshold | No exceptions noted. |
| | | Operating system audit logging configurations are in place that include user activity and system events. | Inspected the operating system audit log configurations to determine that operating system audit logging configurations were in place that included user activity and system events. | No exceptions noted. |
| | | Operating system audit logs are maintained and available for review when needed. | Inquired of the Information Security Director regarding the operating system audit logs to determine that operating system audit logs were maintained and available for review when needed. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and available for review when needed. | No exceptions noted. |
| | **Database - PostgreSQL** | | | |
| | | Databases user access is restricted via role-based security privileges defined within the access control system. | Inspected the databases user listing and access roles to determine that databases user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Databases administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the databases to determine that databases administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the databases administrator listing and access roles to determine that databases administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Databases users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that databases users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Databases account lockout configurations are in place that include:<br>• Account lockout duration<br>• Account lockout threshold | Inspected the databases account lockout configurations to determine that databases account lockout configurations were in place that included:<br>• Account lockout duration<br>• Account lockout threshold | No exceptions noted. |
| | | Databases audit logging configurations are in place to log user activity and system events. | Inspected the databases audit logging configurations to determine that databases audit logging configurations were in place to log user activity and system events. | No exceptions noted. |
| | | Databases audit logs are maintained and available for review when needed. | Inquired of the Information Security Director regarding the databases audit logs to determine that the databases audit logs were maintained and available for review when needed. | No exceptions noted. |
| | | | Inspected an example database audit log extract to determine that databases audit logs were maintained and available for review when needed. | No exceptions noted. |
| | **Application - Helix Platform** | | | |
| | | Application user access is restricted via role-based security privileges defined within the access control system. | Inspected the application user listing and access roles to determine that application user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Application administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the application to determine that application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the application administrator listing and access roles to determine that application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Application users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that application users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |
| | | Application account lockout configurations are in place that include:<br>• Account lockout duration<br>• Account lockout threshold | Inspected the application account lockout configurations to determine that application account lockout configurations were in place that included:<br>• Account lockout duration<br>• Account lockout threshold | No exceptions noted. |
| | | Application audit logging configurations are in place to log user activity and system events. | Inspected the application audit logging configurations to determine that application audit logging configurations were in place to log user activity and system events. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Application audit logs are maintained and available for review when needed. | Inquired of the Information Security Director regarding the application audit logs to determine that application audit logs were maintained and available for review when needed. | No exceptions noted. |
| | | | Inspected an example application audit log extract to determine that application audit logs were maintained and available for review when needed. | No exceptions noted. |
| | **VPN Connection - Cisco AnyConnect** | | | |
| | | VPN user access is restricted via role-based security privileges defined within the access control system. | Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | The ability to administer VPN access is restricted to user accounts accessible by authorized personnel. | Inquired of the Information Security Director regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| | | | Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| Logical and Physical Access | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system. | Inquired of the Information Security Director regarding VPN Access to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |
| | | | Observed a user authenticate to the VPN access to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |
| | | Data coming into the environment is secured and monitored through the use of firewalls and an IDS. | Inspected the IDS configurations, firewall rulesets for the production environment and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDS. | No exceptions noted. |
| | | Critical data is stored in encrypted format using software supporting the AES256. | Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES256. | No exceptions noted. |
| | | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| Logical and Physical Access | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |
| | | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inquired of the Information Security Director regarding new hire access to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | | Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired of the Information Security Director regarding logical access removal to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions 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. | Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. | Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring. | No exceptions noted. |
| | | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inquired of the Information Security Director regarding new hire access to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | | Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired of the Information Security Director regarding logical access removal to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions 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. | Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. | Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring. | No exceptions noted. |
| | | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inquired of the Information Security Director regarding new hire access to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | | Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired of the Information Security Director regarding logical access removal to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |
| CC6.4 | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. | The controls related to this criterion are the responsibility of the subservice organizations. Please refer to the Subservice Organizations section of this report for the controls managed by the subservice organization. | Not applicable. | Not applicable. |
| 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. | Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. | Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction. | No exceptions noted. |
| | | Data that is no longer required for business purposes is rendered unreadable. | Inspected the data disposal and destruction policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the service ticket and certificate of destruction for a sample of data disposals to determine that data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| | | Policies and procedures are in place for removal of media storing critical data or software. | Inspected the SaaS media protection policies and procedures to determine that policies and procedures were in place for removal of media storing critical data or software. | No exceptions noted. |
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | Network address translation (NAT) functionality is utilized to manage internal IP addresses. | Inspected the Network Diagram and NAT rules to determine that NAT functionality was utilized to manage internal IP addresses. | No exceptions noted. |
| | | TLS, VPN and other encryption technologies are used for defined points of connectivity. | Inspected the encryption configurations and digital certificates to determine that TLS, VPN and other encryption technologies were used for defined points of connectivity. | No exceptions noted. |
| | | Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. | Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. | No exceptions noted. |
| | | A firewall is in place to filter unauthorized inbound network traffic from the Internet. | Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the firewall ruleset for the production environment to production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. | Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| | | An IDS is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | | Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | The IDS is configured to notify personnel upon intrusion prevention. | Inspected an example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. | Inspected the antivirus software dashboard console and configurations to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software. | No exceptions noted. |
| | | The antivirus software provider pushes updates automatically to the installed antivirus software as new updates are available. | Inspected the antivirus software dashboard console and configurations to determine that the antivirus software provider pushed updates automatically to the installed antivirus software as new updates were available. | No exceptions noted. |
| | | The antivirus software is configured to scan workstations on a weekly basis. | Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations on a weekly basis. | No exceptions noted. |
| | | Critical data is stored in encrypted format using software supporting the AES256. | Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES256. | No exceptions 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. | Logical access to stored data is restricted to authorized personnel. | Inquired of the Information Security Director regarding logical access to stored data to determine that logical access to stored data was restricted to authorized personnel. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| Logical and Physical Access | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the database user listing and access rights to determine that access to stored data was restricted to authorized personnel. | No exceptions noted. |
| | | Backups are stored in pairs, with data replicated between sites, and an archiving third location offsite. | Inspected the backup configurations and backup logs to determine that backups were stored in pairs, with data replicated between sites, and an archiving third location offsite. | No exceptions noted. |
| | | Backups are completed in a defined frequency and monitored to run successfully. | Inspected the backup configurations and backup logs to determine that backups were completed in a defined frequency and monitored to run successfully. | No exceptions noted. |
| | | The entity secures its environment using a multi-layered defense approach that includes firewalls, an IDS, antivirus software and a DMZ. | Inspected the network diagram, IDS configurations, firewall ruleset for the production environment, and antivirus configurations to determine that the entity secures its environment using a multi-layered defense approach that included firewalls, an IPS, antivirus software and a DMZ. | No exceptions noted. |
| | | TLS, VPN and other encryption technologies are used for defined points of connectivity. | Inspected the encryption configurations and digital certificates to determine that TLS, VPN and other encryption technologies were used for defined points of connectivity. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. | Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. | No exceptions noted. |
| | | A firewall is in place to filter unauthorized inbound network traffic from the Internet. | Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. | Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | An IDS is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | | Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | The IDS is configured to notify personnel upon intrusion prevention. | Inspected an example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |
| | | Backup media is stored in an encrypted format. | Inspected the encryption configurations for backup media to determine that backup media was stored in an encrypted format. | No exceptions noted. |
| | | Use of removable media is prohibited by policy and system configurations except when authorized by management. | Inspected the removable media policies and procedures and configurations to determine that the use of removable media was prohibited by policy and system configurations except when authorized by management. | No exceptions 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. | A warning notification appears when an employee attempted to download an application or software. | Inspected the denial notification to determine that a warning notification appeared when an employee attempted to download an application or software. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Logical and Physical Access** | | | | |
| **CC6.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. | Inspected the antivirus software dashboard console and configurations to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software. | No exceptions noted. |
| | | The antivirus software provider pushes updates automatically to the installed antivirus software as new updates are available. | Inspected the antivirus software dashboard console and configurations to determine that the antivirus software provider pushed updates automatically to the installed antivirus software as new updates were available. | No exceptions noted. |
| | | The antivirus software is configured to scan workstations on a weekly basis. | Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations on a weekly basis. | No exceptions noted. |
| | | An IDS is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | | Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | The IDS is configured to notify personnel upon intrusion prevention. | Inspected an example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Management has defined configuration standards in the information security policies and procedures. | Inspected the information security policies and procedures to determine that management had defined configuration standards in the information security policies and procedures. | No exceptions noted. |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | The monitoring software is configured to alert IT personnel when thresholds have been exceeded. | Inspected the monitoring tool configurations and an example alert to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded. | No exceptions noted. |
| | | An IDS is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | | Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The IDS is configured to notify personnel upon intrusion prevention. | Inspected an example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |
| | | A firewall is in place to filter unauthorized inbound network traffic from the Internet. | Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. | Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | Inspected the information security and the incident response policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | No exceptions noted. |
| | | Vulnerability scans and penetration tests are performed and remedial actions are taken where necessary. | Inspected the completed vulnerability scan results for a sample of quarters and completed penetration test results to determine that vulnerability scans and penetration tests were performed and remedial actions were taken where necessary. | No exceptions noted. |
| CC7.2 | The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | Inspected the information security and the incident response policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | No exceptions noted. |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The monitoring software is configured to alert IT personnel when thresholds have been exceeded. | Inspected the monitoring tool configurations and an example alert to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded. | No exceptions noted. |
| | | An IDS is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | | Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| | | The IDS is configured to notify personnel upon intrusion prevention. | Inspected an example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |
| | | A firewall is in place to filter unauthorized inbound network traffic from the Internet. | Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. | Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| | | | Inspected the firewall ruleset for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| | | Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. | Inspected the antivirus software dashboard console and configurations to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software. | No exceptions noted. |
| | | The antivirus software provider pushes updates automatically to the installed antivirus software as new updates are available. | Inspected the antivirus software dashboard console and configurations to determine that the antivirus software provider pushed updates automatically to the installed antivirus software as new updates were available. | No exceptions noted. |
| | | The antivirus software is configured to scan workstations on a weekly basis. | Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations on a weekly basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |
| 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. | Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| | | The incident response and escalation procedures are reviewed annually for effectiveness. | Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed annually for effectiveness. | No exceptions noted. |
| | | Resolution of incidents are documented within the ticket and communicated to affected users. | Inspected the supporting incident tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users. | No exceptions noted. |
| | | Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | Inspected the supporting incident tickets for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Identified incidents are reviewed, monitored and investigated by an incident response team. | Inspected the supporting incident tickets for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team. | No exceptions noted. |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. | Inquired of the Information Security Director regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | Testing of the control activity disclosed that there were no critical incidents during the review period. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. | Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. | No exceptions 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. | Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. | Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented. | No exceptions noted. |
| | | Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| | | Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | Inspected the supporting incident tickets for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The actions taken to address identified security incidents are documented and communicated to affected parties. | Inspected the supporting incident tickets for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties. | No exceptions noted. |
| | | Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents. | No exceptions noted. |
| | | Resolution of incidents are documented within the ticket and communicated to affected users. | Inspected the supporting incident tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users. | No exceptions noted. |
| | | Remediation actions taken for security incidents are documented within the ticket and communicated to affected users. | Inspected the supporting incident tickets for a sample of incidents to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. | Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. | No exceptions noted. |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. | Inquired of the Information Security Director regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | Testing of the control activity disclosed that there were no critical incidents during the review period. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to:<br>• Rebuilding systems<br>• Updating software<br>• Installing patches<br>• Removing unauthorized access<br>• Changing configurations | Inspected the information security, incident response, and change management policies and procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to:<br>• Rebuilding systems<br>• Updating software<br>• Installing patches<br>• Removing unauthorized access<br>• Changing configurations | No exceptions noted. |
| | | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the SaaS contingency planning policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |
| | | Daily backups are replicated to off-site backup folders. | Inspected the backup configurations and backup logs to determine that daily backups were replicated to off-site backup folders. | No exceptions noted. |
| | | Backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that backup restoration tests were performed on an annual basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| System Operations | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. | Inquired of the Information Security Director regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | Testing of the control activity disclosed that there were no critical incidents during the review period. |
| | | A business continuity and contingency plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity and contingency plans to determine that a business continuity and contingency plans were documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | No exceptions noted. |
| | | The business continuity plan is tested on an annual basis. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **System Operations** | | | | |
| **CC7.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The business continuity and contingency plans are updated based on business continuity plan test results. | Inspected the business continuity and contingency plans and completed business continuity and completed test results to determine that the business continuity and contingency plans were updated based on business continuity plan test results. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Change Management** | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Documented change control policies and procedures are in place to guide personnel in the change management process. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process. | No exceptions noted. |
| | | The change management process has defined the following roles and assignments:<br>• Authorization of change requests- Authorized personnel from the Customer<br>• Development - Trained SaaS Personnel<br>• Testing - Trained SaaS Personnel<br>• Implementation - Trained SaaS Personnel | Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments:<br>• Authorization of change requests- Authorized personnel from the Customer<br>• Development - Trained SaaS Personnel<br>• Testing - Trained SaaS Personnel<br>• Implementation - Trained SaaS Personnel | No exceptions noted. |
| | | System changes are communicated to both affected internal and external users. | Inspected the e-mail notification configurations and an example alert template to determine that system changes were communicated to both affected internal and external users. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| Change Management | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Access to implement changes in the production environment is restricted to authorized IT personnel. | Inquired of the Information Security Director regarding the users with access to deploy changes to determine that access to implement changes in the production environment was restricted to authorized IT personnel. | No exceptions noted. |
| | | | Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel. | No exceptions noted. |
| | | System changes are authorized and approved by management prior to implementation. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were authorized and approved by management prior to implementation. | No exceptions noted. |
| | | Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. | Inspected the change control software configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Change Management** | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Development and test environments are physically and logically separated from the production environment. | Inspected the separate development, QA, and production environments to determine that development and test environments were physically and logically separated from the production environment. | No exceptions noted. |
| | | System change requests are documented and tracked in a ticketing system. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system change requests were documented and tracked in a ticketing system. | No exceptions noted. |
| | | Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation. | No exceptions noted. |
| | | System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Change Management** | | | | |
| **CC8.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Information security policies and procedures document the baseline requirements for the configuration of IT systems and tools. | Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for the configuration of IT systems and tools. | No exceptions noted. |
| | | Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. | Inspected the risk management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities. | No exceptions noted. |
| | | Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances. | Inspected the risk management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances. | No exceptions noted. |
| | | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inquired of the Information Security Director regarding the risk register to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |
| | | | Observed the risk register to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the internal risk audit to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |
| | | Identified risks are rated using a risk evaluation process and ratings are approved by management. | Inquired of the Information Security Director regarding the risk register to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | | Observed the risk register to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | Management develops risk mitigation strategies to address risks identified during the risk assessment process. | Inquired of the Information Security Director regarding the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Observed the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |
| | | | Inspected the risk management policies and procedures and the internal risk audit to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |
| | | The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability. | Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability. | No exceptions noted. |
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. | Inspected the procurement policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. | Inquired of the Information Security Director regarding third-party risks to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process. | No exceptions noted. |
| | | | Inspected the vendor risk assessment review for a sample of third-parties to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process. | No exceptions noted. |
| | | The entity's third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties. | Inspected the third-party agreement template to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties. | No exceptions noted. |
| | | | Inspected the executed third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|---|---|---|
| **Risk Mitigation** | | | | |
| **CC9.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | Inspected the completed third-party attestation report for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | No exceptions noted. |
| | | The entity's third-party agreement outlines and communicates confidentiality commitments and requirements. | Inspected the third-party agreement template to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements. | No exceptions noted. |
| | | | Inspected the executed third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| 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. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | The monitoring software is configured to alert IT personnel when thresholds have been exceeded. | Inspected the monitoring tool configurations and an example alert to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded. | No exceptions noted. |
| | | Processing capacity is monitored 24x7x365. | Inspected the monitoring tool configurations and dashboard to determine that processing capacity was monitored 24x7x365. | No exceptions noted. |
| | | Future processing demand is forecasted and compared to scheduled capacity on an annual basis. | Inspected the capacity optimization reports to determine that future processing demand was forecasted and compared to scheduled capacity on an annual basis. | No exceptions 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. | Backups are stored in pairs, with data replicated between sites, and an archiving third location offsite. | Inspected the backup configurations and backup logs to determine that backups were stored in pairs, with data replicated between sites, and an archiving third location offsite. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Backups are completed and monitored to run successfully. | Inspected the backup configurations and logs to determine that backups were completed and monitored to run successfully. | No exceptions noted. |
| | | Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable. | Inspected the business continuity and contingency plans and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable. | No exceptions noted. |
| | | Additional controls related to this criterion are the responsibility of the subservice organizations. Please see the Subservice Organizations section of this report for additional controls managed by the subservice organizations. | Not applicable. | Not applicable. |
| A1.3 | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. | Inspected the business continuity and contingency plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY | | | | |
|---|---|---|---|---|
| **A1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The business continuity plan is tested on an annual basis and includes:<br>• Various testing scenarios based on threat likelihood<br>• Identifying the critical systems required for business operations<br>• Assigning roles and responsibilities in the event of a disaster<br>• Assessing and mitigating risks identified as a result of the test disaster | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis and included:<br>• Various testing scenarios based on threat likelihood<br>• Identifying the critical systems required for business operations<br>• Assigning roles and responsibilities in the event of a disaster<br>• Assessing and mitigating risks identified as a result of the test disaster | No exceptions noted. |
| | | Backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that backup restoration tests were performed on an annual basis. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY | | | | |
|---|---|---|---|---|
| **C1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| C1.1 | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | Documented confidential policies and procedures are in place that included:<br>• Defining, identifying, and designating information as confidential<br>• Storing confidential information<br>• Protecting confidential information from erasure or destruction<br>• Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed | Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place that included:<br>• Defining, identifying, and designating information as confidential<br>• Storing confidential information<br>• Protecting confidential information from erasure or destruction<br>• Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed | No exceptions noted. |
| | | An inventory log is maintained of assets with confidential data. | Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data. | No exceptions noted. |
| | | Confidential information is maintained in locations restricted to those authorized to access. | Inquired of the Information Security Director regarding confidential information to determine that confidential information was maintained in locations restricted to those authorized to access. | No exceptions noted. |
| | | | Inspected the file access permissions for an example file marked as confidential to determine that confidential information was maintained in locations restricted to those authorized to access. | No exceptions noted. |

| ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY | | | | |
|---|---|---|---|---|
| **C1.0** | **Criteria** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| C1.2 | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | Documented data destruction policies and procedures are in place that included:<br>• Identifying confidential information requiring destruction when the end of the retention period is reached<br>• Erasing or destroying confidential information that has been identified for destruction | Inspected the media protection policies and procedures to determine that documented data destruction policies and procedures were in place that included:<br>• Identifying confidential information requiring destruction when the end of the retention period was reached<br>• Erasing or destroying confidential information that has been identified for destruction | No exceptions noted. |
| | | An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged. | Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged. | No exceptions noted. |
| | | The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed. | Inspected the destruction certificate for a sample of requests to dispose of data to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed. | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OIS-01 | The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organizational units, locations, and procedures for providing the cloud service.<br>The measures for setting up, implementing, maintaining, and continuously improving the ISMS are documented.<br>The documentation includes:<br>• Scope of the ISMS (Section 4.3 of ISO/IEC 27001)<br>• Declaration of applicability (Section 6.1.3)<br>• Results of the last management review (Section 9.3) | The entity's internal controls framework is based on a recognized (ISO/IEC 27001) framework.<br><br>Policies for setting up, implementing, maintaining, and continuously improving the ISMS are documented and updated on an annual basis. | Inspected the compliance reports and completed internal controls matrix to determine that the entity's internal controls framework was based on a recognized (ISO/IEC 27001) framework.<br><br>Inquired of the Information Security Director regarding change implementation to determine that policies for setting up, implementing, maintaining, and continuously improving the ISMS were documented and updated on an annual basis.<br><br>Inspected the company's policies and procedures including revision history to determine that policies for setting up, implementing, maintaining, and continuously improving the ISMS were documented and updated on an annual basis. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OIS-02 | The top management of the Cloud Service Provider has adopted an information security policies and procedures and communicated it to internal and external employees as well as cloud customers.<br>The policy describes:<br>• The importance of information security, based on the requirements of cloud customers in relation to information security<br>• The security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider<br>• The most important aspects of the security strategy to achieve the security objectives set<br>• The organizational structure for information security in the ISMS application area | Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.<br><br>Relevant information security policies and procedures are made available to relevant users. | Inspected the information security policies and procedures, the SaaS roles and responsibilities, and the entity's shared drive to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.<br><br>Inspected the front-facing company website to determine that relevant information security policies and procedures were made available to relevant users. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OIS-03 | Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third-parties are documented and communicated. This includes dealing with the following events:<br>• Vulnerabilities<br>• Security incidents<br>• Malfunctions<br><br>The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organizations in order to carry out the activities appropriately (e.g., definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts).<br><br>The communication of changes to the interfaces and dependencies takes place in a timely manner so that the affected organizations and third-parties can react appropriately with organizational and technical measures before the changes take effect. | A third-party agreement communicates the system commitments and requirements of third-parties. | Inspected the executed third-party agreement for a sample of third-parties to determine that a third-party agreement communicated the system commitments and requirements of third-parties. | No exceptions noted. |
| | | Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment. | Inspected the vulnerability management process policies and procedures to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment. | No exceptions noted. |
| | | Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| | | Business continuity and contingency plans are developed and updated on an annual basis. | Inspected the business continuity and contingency plans to determine that business continuity and contingency plans were developed and updated on an annual basis. | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OIS-04 | Conflicting tasks and responsibilities are separated based on an OIS-06 risk assessment to reduce the risk of unauthorized or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service. | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |
| | The risk assessment covers the following areas, insofar as these are applicable to the provision of the Cloud Service and are in the area of responsibility of the Cloud Service Provider:<br>• Administration of rights profiles, approval and assignment of access and access authorizations (cf. IDM-01)<br>• Development, testing and release of changes (cf. DEV-01)<br>• Operation of the system components<br><br>If separation cannot be established for organizational or technical reasons, measures are in place to monitor the activities in order to detect unauthorized or unintended changes as well as misuse and to take appropriate actions. | The entity's risk assessment process includes:<br>• Identifying the relevant information assets that are critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that the entity's risk assessment process included:<br>• Identifying the relevant information assets that were critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |
| | | Administration of rights profiles, approval and assignment of access and access authorizations are evaluated as a part of the annual risk assessment process. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that administration of rights profiles, approval and assignment of access and access authorizations were evaluated as a part of the annual risk assessment process. | No exceptions noted. |
| | | File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. | Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes were deployed into the production environment. | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |
| OIS-05 | The Cloud Service Provider leverages relevant authorities and interest groups in order to stay informed about current threats and vulnerabilities. The information flows into the procedures for handling risks (cf. OIS-06) and vulnerabilities (cf. OPS-19). | Key personnel attend information security events to keep up to date with latest developments and trends in information security. | Inspected the ISPMS Management Review to determine that key personnel attended information security events to keep up to date with latest developments and trends in information security. | No exceptions noted. |
| | | Management follows a methodical process to identify assets, associated threats and vulnerabilities, and quantified the probability, and harm that could be inflicted. | Inspected the completed risk assessment to determine that management followed a methodical process to identify assets, associated threats and vulnerabilities, and quantified the probability, and harm that could be inflicted. | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OIS-06 | Policies and instructions for risk management procedures are documented, communicated, and provided in accordance with SP-01 for the following aspects:<br>• Identification of risks associated with the loss of confidentiality, integrity, availability, and authenticity of information within the scope of the ISMS and assigning risk owners<br>• Analysis of the probability and impact of occurrence and determination of the level of risk<br>• Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritization of handling<br>• Handling of risks through measures, including approval of authorization and acceptance of residual risks by risk owners<br>• Documentation of the activities implemented to enable consistent, valid and comparable results | The entity's risk assessment process includes:<br>• Identifying the relevant information assets that are critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks<br>• Identified for each identified vulnerability | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that the entity's risk assessment process included:<br>• Identifying the relevant information assets that were critical to business operations<br>• Prioritizing the criticality of those relevant information assets<br>• Identifying and assessing the impact of the threats to those information assets<br>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats<br>• Assessing the likelihood of identified threats and vulnerabilities<br>• Determining the risks associated with the information assets<br>• Addressing the associated risks<br>• Identified for each identified vulnerability | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Identified risks are rated using a risk evaluation process and ratings are approved by management. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management. | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OIS-07 | The Cloud Service Provider executes the process for handling risks as needed or at least once a year. The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider:<br>• Processing, storage or transmission of data of cloud customers with different protection needs<br>• Occurrence of weak points and malfunctions in technical protective measures for separating shared resources<br>• Attacks via access points, including interfaces accessible from public networks<br>• Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons<br>• Dependencies on subservice organizations<br><br>The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed for adequacy at least annually by the risk owners. | The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards. | Inspected the ISO Certification to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations, and standards. | No exceptions noted. |
| | | Management develops risk mitigation strategies to address risks identified during the risk assessment process. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |
| | | For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities. | No exceptions noted. |
| | | The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. | Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management. | No exceptions noted. |

| CONTROL DOMAIN: ORGANISATION OF INFORMATION SECURITY (OIS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties. | Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed on an annual basis which included reviewing activities performed by third-parties. | No exceptions noted. |

| CONTROL DOMAIN: SECURITY POLICIES AND INSTRUCTIONS (SP) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SP-01 | Policies and instructions (incl. concepts and guidelines) are derived from the information security policies and procedures and are documented according to a uniform structure. They are communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner.<br><br>The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorized body.<br><br>The policies and instructions describe at least the following aspects:<br>• Objectives<br>• Scope<br>• Roles and responsibilities, including staff qualification requirements and the establishment of substitution rules<br>• Roles and dependencies on other organizations (especially cloud customers and subservice organizations)<br>• Steps for the execution of the security strategy<br>• Applicable legal and regulatory requirements | Organizational and information security policies and procedures are documented and made available to employee's through the entity's shared drive.<br><br>Relevant information security policies and procedures are made available to cloud customers. | Inspected the information security policies and procedures and the entity's shared drive to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's shared drive.<br><br>Inspected the front-facing company website to determine that relevant information security policies and procedures were made available to cloud customers. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: SECURITY POLICIES AND INSTRUCTIONS (SP) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SP-02 | Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider's subject matter experts.<br><br>The review shall consider at least the following aspects:<br>• Organizational and technical changes in the procedures for providing the cloud service<br>• Legal and regulatory changes in the Cloud Service Provider's environment<br><br>Revised policies and instructions are approved before they become effective. | The information security policies and procedures is reviewed on an annual basis by management and accounts for any changes to organizational, technical or legal requirements. | Inspected the information security policies and procedures including revision history to determine that the information security policies and procedures was reviewed on an annual basis by management and accounted for any changes to organizational, technical, or legal requirements. | No exceptions noted. |
| SP-03 | Exceptions to the policies and instructions for information security as well as respective controls go through the OIS-06 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of exceptions are documented, limited in time and are reviewed for appropriateness at least annually by the risk owners. | Accepted risks identified during the risk assessment process are documented and reviewed for appropriateness by management on an annual basis. | Inspected the issue tracker to determine that accepted risks identified during the risk assessment process were documented and reviewed for appropriateness by management on an annual basis. | No exceptions noted. |

| CONTROL DOMAIN: PERSONNEL (HR) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| HR-01 | The competency and integrity of all internal and external employees of the Cloud Service Provider with access to cloud customer data or system components under the Cloud Service Provider's responsibility who are responsible to provide the cloud service in the production environment shall be verified prior to commencement of employment in accordance with local legislation and regulation by the Cloud Service Provider.<br><br>To the extent permitted by law, the review will cover the following areas:<br>• Verification of the person through identity card<br>• Verification of the CV<br>• Verification of academic titles and degrees.<br>• Request of a police clearance certificate for applicants<br>• Certificate of good conduct or national equivalent<br>• Evaluation of the risk to be blackmailed | Upon hire, personnel are required to complete a background check.<br><br>The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.<br><br>Prior to hire, the entity evaluates all job applicants by reviewing the following articles:<br>• Identification card<br>• Current resume<br>• Verification of academic titles and degrees<br>• Background checks<br>• Certificate of good conduct or national equivalent | Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.<br><br>Inspected the documented interview questionnaire for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.<br><br>Inquired of the information security director regarding recruiting to determine that prior to hire, the entity evaluated all job applicants by reviewing the following articles:<br>• Identification Card<br>• Current resume<br>• Verification of academic titles and degrees<br>• Background checks<br>• Certificate of good conduct or national equivalent | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: PERSONNEL (HR) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the documented interview questionnaire, for a sample of new hires to determine that prior to hire, the entity evaluated all job applicants by reviewing the following articles:<br>• Identification Card<br>• Current resume<br>• Verification of academic titles and degrees<br>• Background checks<br>• Certificate of good conduct or national equivalent | No exceptions noted. |
| HR-02 | The Cloud Service Provider's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security. | Employees are required to acknowledge the confidentiality policies and procedures upon hire. | Inspected the signed confidentiality agreement for a sample of new hires to determine that employees were required to acknowledge the confidentiality policies and procedures upon hire. | No exceptions noted. |
| | The information security policies and procedures, and the policies and instructions based on it, are to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment. | The entity's confidentiality requirements are evaluated on an annual basis and updated if needed. | Inspected the confidentiality policies and procedures with revision history to determine that the entity's confidentiality requirements were evaluated on an annual basis and updated if needed. | No exceptions noted. |

| CONTROL DOMAIN: PERSONNEL (HR) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | Inspected the signed employee code of conduct acknowledgement, and information security and awareness training completion form for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | No exceptions noted. |

| CONTROL DOMAIN: PERSONNEL (HR) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| HR-03 | The Cloud Service Provider operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the Cloud Service Provider on a regular basis. The program is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects:<br>• Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures<br>• Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements<br>• Information about the current threat situation<br>• Correct behavior in the event of security incidents | Executive management has created a training program for its employees. | Inspected the information security and awareness training program to determine that executive management created a training program for its employees. | No exceptions noted. |
| | | Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | Inspected the signed employee code of conduct acknowledgement, and information security and awareness training completion form for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | No exceptions noted. |
| | | Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | Inspected the signed employee code of conduct acknowledgement, and information security and awareness training completion form a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | No exceptions noted. |

| CONTROL DOMAIN: PERSONNEL (HR) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| HR-04 | In the event of violations of policies and instructions or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects:<br>• Verifying whether a violation has occurred<br>• Consideration of the nature and severity of the violation and its impact<br><br>The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures.<br><br>The use of disciplinary measures is appropriately documented. | Sanction policies, which include suspension and termination, are in place for employee misconduct or violation of the entity's policies and procedures. | Inspected the sanction policies and procedures to determine that sanction policies, which include suspension and termination, were in place for employee misconduct or violation of the entity's policies and procedures. | No exceptions noted. |
| HR-05 | Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. | Employees are required to acknowledge the confidentiality policies and procedures upon hire. | Inspected the signed confidentiality agreement for a sample of new hires to determine that employees were required to acknowledge the confidentiality policies and procedures upon hire. | No exceptions noted. |
| | | The entity's confidentiality requirements are evaluated on an annual basis and updated if needed. | Inspected the confidentiality policies and procedures with revision history to determine that the entity's confidentiality requirements were evaluated on an annual basis and updated if needed. | No exceptions noted. |

| CONTROL DOMAIN: PERSONNEL (HR) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| HR-06 | The non-disclosure or confidentiality agreements to be agreed with internal employees, external service providers and suppliers of the Cloud Service Provider are based on the requirements identified by the Cloud Service Provider for the protection of confidential information and operational details.<br><br>The agreements are to be accepted by external service providers and suppliers when the contract is agreed. The agreements must be accepted by internal employees of the Cloud Service Provider before authorization to access data of cloud customers is granted.<br><br>The requirements must be documented and reviewed at regular intervals (at least annually). If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated.<br><br>The Cloud Service Provider must inform the internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement. | Employees are required to acknowledge the confidentiality policies and procedures upon hire.<br><br>A third-party agreement communicates the confidentiality commitments and requirements of third-parties.<br><br>Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via website releases.<br><br>Confidentiality requirements of external parties are reviewed by management on an annual basis and update if needed. | Inspected the signed confidentiality agreement for a sample of new hires to determine that employees were required to acknowledge the confidentiality policies and procedures upon hire.<br><br>Inspected the executed third-party agreement for a sample of third-parties to determine that a third-party agreement communicated the confidentiality commitments and requirements of third-parties.<br><br>Inspected the entity's release calendar to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users, and customers via website releases.<br><br>Inspected the confidentiality policies and procedures including revision history to determine that confidentiality requirements of external parties were reviewed by management on an annual basis and update if needed. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: ASSET MANAGEMENT (AM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| AM-01 | The Cloud Service Provider has established procedures for inventorying assets.<br><br>The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid, and consistent inventory throughout the asset lifecycle.<br><br>Assets are recorded with the information needed to apply the Risk Management Procedure (Cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle. Changes to this information are logged. | The entity has defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors.<br><br>An inventory of system assets and components is maintained to classify and manage the information assets. | Inspected the confidential information protection policies and procedures to determine that the entity had defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors.<br><br>Inspected the inventory listing of system assets and components to determine an inventory of system assets and components was maintained to classify and manage the information assets. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: ASSET MANAGEMENT (AM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| AM-02 | Policies and instructions for acceptable use and safe handling of assets are documented, communicated, and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset:<br>• Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorized personnel or system components<br>• Inventory<br>• Classification and labelling based on the need for protection of the information and measures for the level of protection identified<br>• Secure configuration of mechanisms for error handling, logging, encryption, authentication, and authorization<br>• Requirements for versions of software and images as well as application of patches<br>• Handling of software for which support, and security patches are not available anymore<br><br>**Continues on the next page.* | The entity has defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors.<br><br>The organization has defined acceptable use policy for organizationally owned mobile devices. Installation of unapproved applications was prohibited.<br><br>Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. | Inspected the confidential information protection policies and procedures to determine that the entity had defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors.<br><br>Inspected the communication systems user and security policy to determine that the organization had defined acceptable use for organizationally owned mobile devices, and that installation of unapproved applications was prohibited.<br><br>Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: ASSET MANAGEMENT (AM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Restriction of software installations or use of services<br>• Protection against malware<br>• Remote deactivation, deletion, or blocking<br>• Physical delivery and transport<br>• Dealing with incidents and vulnerabilities<br>• Complete and irrevocable deletion of the data upon decommissioning | | | |
| AM-03 | The Cloud Service Provider has an approval process for the use of hardware to be commissioned, which is used to provide the cloud service in the production environment, in which the risks arising from the commissioning are identified, analyzed, and mitigated. Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication, and authorization according to the intended use and based on the applicable policies. | Organizationally owned systems are configured to management approved standards or requirements prior to being commissioned. | Inspected the information security policies and procedures to determine that all organizationally owned systems were configured to management approved standards or requirements prior to being commissioned. | No exceptions noted. |

| CONTROL DOMAIN: ASSET MANAGEMENT (AM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| AM-04 | The decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the Cloud Service Provider requires approval based on the applicable policies. | Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. | Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction. | No exceptions noted. |
| | The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media. | Data that is no longer required for business purposes is rendered unreadable. | Inspected the data disposal and destruction policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| | | | Inspected the service ticket and certificate of destruction for a sample of data disposals to determine that data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| AM-05 | The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorized access could compromise the information security of the Cloud Service. | Employees are required to acknowledge the acceptable-use policies and procedures upon hire. | Inspected the signed confidentiality policies and procedures for a sample of new hires to determine that employees were required to acknowledge the acceptable-use policies and procedures upon hire. | No exceptions noted. |
| | Any assets handed over are provably returned upon termination of employment. | Logical access to systems is revoked and all company-owned assets are returned as a component of the termination process. | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked and all company-owned assets were returned as a component of the termination process. | No exceptions noted. |

| CONTROL DOMAIN: ASSET MANAGEMENT (AM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| AM-06 | Assets are classified and, if possible, labelled. Classification and labelling of an asset reflects the protection needs of the information it processes, stores, or transmits.<br><br>The need for protection is determined by the individuals or groups responsible for the assets of the Cloud Service Provider according to a uniform schema. The schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. | The entity has defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors.<br><br>An inventory of system assets and components is maintained to classify and manage the information assets. | Inspected the confidential information protection policies and procedures to determine that the entity had defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors.<br><br>Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PS-01 | Security requirements for premises and buildings related to the cloud service provided, are based on the security objectives of the information security policies and procedures, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The security requirements are documented, communicated and provided in a policy or concept according to SP-01.<br><br>The security requirements for data centers are based on criteria which comply with established rules of technology. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements:<br>• Faults in planning<br>• Unauthorized access<br>• Insufficient surveillance<br>• Insufficient air-conditioning<br>• Fire and smoke<br>• Water<br>• Power failure<br>• Air ventilation and filtration<br><br>*Continues on the next page.* | The physical security requirements of critical third-parties are tracked and maintained by management.<br><br>Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Inspected the physical and environmental protection policies and procedures to determine that the physical security requirements of critical third-parties were tracked and maintained by management.<br><br>Not applicable. | No exceptions noted.<br><br>Not applicable. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | If the Cloud Service Provider uses premises or buildings operated by third-parties to provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third-parties.<br><br>The appropriate and effective verification of implementation is carried out in accordance with the criteria for controlling and monitoring subcontractors (cf. SSO-01, SSO-02). | | | |
| PS-02 | The cloud service is provided from two locations that are redundant to each other. The locations meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and are located in an adequate distance to each other to achieve operational redundancy. Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 - Verification, updating and testing of business continuity). | Geographic redundancy is built into the infrastructure through the utilization of third-party data centers in geographically dispersed, disaster-neutral locations. | Inquired of the Information Security Director regarding geographic redundancy to determine that geographic redundancy was built into the infrastructure through the utilization of third-party data centers in geographically dispersed, disaster-neutral locations. | No exceptions noted. |
| | | | Inspected the network diagram and business continuity plan to determine that geographic redundancy was built into the infrastructure through the utilization of third-party data centers in geographically dispersed, disaster-neutral locations. | No exceptions noted. |
| | | Backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that backup restoration tests were performed on an annual basis. | No exceptions noted. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The business continuity plan is tested on an annual basis. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted. |
| PS-03 | The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept).<br><br>The security measures are designed to detect and prevent unauthorized access in a timely manner so that it does not compromise the information security of the cloud service.<br><br>The outer doors, windows and other construction elements reach a level appropriate to the security requirements and withstand a burglary attempt for at least 10 minutes.<br><br>The surrounding wall constructions as well as the locking mechanisms meet the associated requirements. | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PS-04 | At access points to premises and buildings related to the cloud service provided, physical access controls are set up in accordance with the Cloud Service Provider's security requirements (cf. PS-01 Security Concept) to prevent unauthorized access.<br><br>Access controls are supported by an access control system.<br><br>The requirements for the access control system are documented, communicated and provided in a policy or concept in accordance with SP-01 and include the following aspects:<br>• Specified procedure for the granting and revoking of access authorizations (cf. IDM-02) based on the principle of least authorization ("least-privilege-principle") and as necessary for the performance of tasks ("need-to-know-principle")<br>• Automatic revocation of access authorizations if they have not been used for a period of 2 month<br>• Automatic withdrawal of access authorizations if they have not been used for a period of 6 months<br><br>*Continues on the next page.* | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Two-factor authentication for access to areas hosting system components that process cloud customer information<br>• Visitors and external personnel are tracked individually by the access control during their work in the premises and buildings, identified as such (e.g., by visible wearing of a visitor pass) and supervised during their stay<br>• Existence and nature of access logging that enables the Cloud Service Provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided | | | |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PS-05 | Premises and buildings related to the cloud service provided are protected from fire and smoke by structural, technical and organizational measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and include the following aspects:<br>• Structural Measures:<br>  ○ Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts<br>• Technical Measures:<br>  ○ Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided<br><br>*Continues on the next page.* | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | ○ Extinguishing system or oxygen reduction<br>○ Fire alarm system with reporting to the local fire department<br>• Organizational Measures:<br>○ Regular fire protection inspections to check compliance with fire protection requirements<br>○ Regular fire protection exercises | | | |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PS-06 | Measures to prevent the failure of the technical supply facilities required for the operation of system components with which information from cloud customers is processed, are documented and set up in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) with respect to the following aspects:<br>• Operational redundancy (N+1) in power and cooling supply<br>• Use of appropriately sized uninterruptible power supplies (UPS) and emergency power systems (NEA), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPS and NEA is checked at least annually by suitable tests and exercises (cf. BCM-04 -Verification, updating and testing of business continuity)<br>• Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations<br><br>*Continues on the next page.* | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping. The protection is checked regularly, but at least every two years, as well as in case of suspected manipulation by qualified personnel regarding the following aspects:<br>○ Traces of violent attempts to open closed distributors<br>○ Up-to-datedness of the documentation in the distribution list<br>○ Conformity of the actual wiring and patching with the documentation<br>○ The short-circuits and earthing of unneeded cables are intact<br>○ Impermissible installations and modifications | | | |

| CONTROL DOMAIN: PHYSICAL SECURITY (PS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PS-07 | The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). When the permitted control range is exceeded, the responsible departments of the Cloud-Provider are automatically informed in order to promptly initiate the necessary measures for return to the control range. | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-01 | The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements. | Processing capacity is monitored 24x7x365. | Inspected the monitoring tool configurations and dashboard to determine that processing capacity was monitored 24x7x365. | No exceptions noted. |
| | | Future processing demand is forecasted and compared to scheduled capacity on an annual basis. | Inspected the capacity optimization reports to determine that future processing demand was forecasted and compared to scheduled capacity on an annual basis. | No exceptions noted. |
| OPS-02 | Technical and organizational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Processing capacity is monitored 24x7x365. | Inspected the monitoring tool configurations and dashboard to determine that processing capacity was monitored 24x7x365. | No exceptions noted. |
| | | End-user access to the in-scope application requires a unique username, password combination, and MFA. | Inquired of the Information Security Director regarding application authentication to determine that end-user access to the in-scope application required a unique username, password combination, and MFA. | No exceptions noted. |
| | | | Observed a user authenticate to the in-scope application to determine that end-user access to the in-scope application required a unique username, password combination, and MFA. | No exceptions noted. |
| OPS-03 | Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance. | Not applicable. The entity's service model does not allow for cloud customers to allocate system resources. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-04 | Policies and instructions that provide protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects:<br>• Use of system-specific protection mechanisms<br>• Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment<br>• Operation of protection programs for employees' terminal equipment | Organizational and information security policies and procedures are documented and made available to employee's through the entity's shared drive. | Inspected the information security policies and procedures and the entity's shared drive to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's shared drive. | No exceptions noted. |
| | | Standard Operating Procedures (SOPs) are in place that define system operation requirements mandatory for maintaining the cloud service environment. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment. | No exceptions noted. |
| | | SOPs are reviewed by management on an annual basis. | Inspected the entity's SOPs with the revision history to determine that SOPs were reviewed by management on an annual basis. | No exceptions noted. |
| OPS-05 | System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behavior-based malware detection and removal, these protection programs are updated at least daily. | Anti-malware software solutions are implemented to perform frequent updates and daily scans to prevent the execution of malware. | Inspected the anti-malware configuration to determine that the anti-malware software solutions were implemented to perform frequent updates and daily scans to prevent the execution of malware. | No exceptions noted. |
| | | The antivirus software provider pushes updates automatically to the installed antivirus software as new updates are available. | Inspected the antivirus software dashboard console and configurations to determine that the antivirus software provider pushed updates automatically to the installed antivirus software as new updates were available. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| OPS-06 | Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects. | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the SaaS contingency planning policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |
| | The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO):<br>• Data is backed up in encrypted, state-of-the-art form<br>• Access to the backed-up data and the execution of restores is performed only by authorized persons<br>• Tests of recovery procedures (cf. OPS-08) | Backup media is stored in an encrypted format. | Inspected the encryption configurations for backup media to determine that backup media was stored in an encrypted format. | No exceptions noted. |
| | | The ability to recall backed up data is restricted to authorized personnel. | Inquired of the Information Security Director regarding the ability to recall backed up data to determine that the ability to recall backed up data was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the list of users with the ability to recall backup media from third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel. | No exceptions noted. |
| | | Data backed up is replicated to an offsite facility real-time. | Inspected the backup replication configurations to determine that data backed up was replicated to an offsite facility in real-time. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that backup restoration tests were performed on an annual basis. | No exceptions noted. |
| | | Backup data that is no longer required for business purposes is rendered unreadable. | Inspected the data disposal and destruction policies and procedures to determine that backup data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| | | Customer data is backed up in accordance with the entity's SaaS contingency planning policies and procedures. | Inspected the customer data processing addendum and backup policies and procedures to determine that customer data was backed up in accordance with the entity's SaaS contingency planning policies and procedures. | No exceptions noted. |
| OPS-07 | The execution of data backups is monitored by technical and organizational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service Provider's business requirements regarding the scope and frequency of data backup and the duration of storage. | Backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that backup restoration tests were performed on an annual basis. | No exceptions noted. |
| | | When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. | Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-08 | Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02).<br><br>Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions. | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the SaaS contingency planning policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |
| | | Data backup restoration test is performed at least annually. | Inspected the completed backup restoration test results to determine that data backup restoration test was performed at least annually. | No exceptions noted. |
| OPS-09 | The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factor's recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site. | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the SaaS contingency planning policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |
| | | Backup media is replicated in real-time to multiple locations. | Inspected the backup policies and procedures and backup configurations to determine that backup media was replicated in real-time to multiple locations. | No exceptions noted. |
| | | Backup media is stored in an encrypted format. | Inspected the backup encryption configurations to determine that backup media was stored in an encrypted format. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Transmission of digital output beyond the boundary of the system is encrypted. | Inspected the encryption configurations for data in transit to determine that transmission of digital output beyond the boundary of the system was encrypted. | No exceptions noted. |
| OPS-10 | The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects:<br>• Definition of events that could lead to a violation of the protection goals<br>• Specifications for activating, stopping and pausing the various logs<br>• Information regarding the purpose and retention period of the logs<br>• Define roles and responsibilities for setting up and monitoring logging<br>• Time synchronization of system components<br>• Compliance with legal and regulatory frameworks | Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | Inspected the information security and the incident response policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | No exceptions noted. |
| | | System clocks for information systems are configured to synchronize to reliable time servers. | Inspected the internal and external time servers defined in the domain name service (DNS) for the production environments to determine that system clocks for information systems were configured to synchronize to reliable time servers. | No exceptions noted. |
| | | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | The entity has defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors. | Inspected the confidential information protection policies and procedures to determine that the entity had defined and adopted data classifications based on data type, sensitivity, criticality, contractual and legal requirements, and other factors. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-11 | Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects:<br>• Metadata is collected and used solely for billing, incident management and security incident management purposes<br>• Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user<br>• No commercial use<br>• Storage for a fixed period reasonably related to the purposes of the collection<br>• Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary<br>• Provision to cloud customers according to contractual agreements | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment.<br><br>Customer metadata is recorded, maintained, and removed based on documented policies and procedures. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment.<br><br>Inspected the confidential information protection and data retention policies and procedures to determine that customer metadata was recorded, maintained, and removed based on documented policies and procedures. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-12 | The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures regarding the following restrictions:<br>• Access only to authorized users and systems<br>• Retention for the specified period<br>• Deletion when further retention is no longer necessary for the purpose of collection | Customer metadata is recorded, maintained, and removed based on documented policies and procedures. | Inspected the confidential information protection and data retention policies and procedures to determine that customer metadata was recorded, maintained, and removed based on documented policies and procedures. | No exceptions noted. |
| | | Database user access is restricted via role-based security privileges defined within the access control system. | Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Databases administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the databases to determine that databases administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the databases administrator listing and access roles to determine that databases administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Databases audit logging configurations are in place to log user activity and system events. | Inspected the databases audit logging configurations to determine that databases audit logging configurations were in place to log user activity and system events. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Customer data that is no longer required for business purposes is rendered unreadable. | Inspected the data disposal and destruction policies and procedures to determine that customer data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| | | | Inspected the destruction certificate for a sample of requests to dispose of data to determine that customer data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| OPS-13 | The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation).<br><br>Identified events are automatically reported to the appropriate departments for prompt evaluation and action. | Application audit logging configurations are in place to log user activity and system events. | Inspected the application audit logging configurations to determine that application audit logging configurations were in place to log user activity and system events. | No exceptions noted. |
| | | Application audit logs are maintained and available for review when needed. | Inquired of the Information Security Director regarding the application audit logs to determine that application audit logs were maintained and available for review when needed. | No exceptions noted. |
| | | | Inspected an example application audit log extract to determine that application audit logs were maintained and available for review when needed. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | The monitoring software is configured to alert IT personnel when thresholds have been exceeded. | Inspected the monitoring tool configurations and an example alert to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded. | No exceptions noted. |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. | Inquired of the Information Security Director regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | Testing of the control activity disclosed that there were no critical incidents during the review period. |
| OPS-14 | The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable, and aggregated form, regardless of the source of such data, so that a central, authorized evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected.<br><br>Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management). | Logs from information systems are aggregated and secured to a central repository. | Inspected the dashboard for log file storage and analysis to determine that logs from information systems were aggregated and secured to a central repository. | No exceptions noted. |
| | | A role-based access control system was utilized to restrict write access to log files to the administrator group members. | Inspected the network administrator group listing to determine that a role-based access control system was utilized to restrict write access to log files to the administrator group members. | No exceptions noted. |
| | | Log data is immutable and cannot be modified. | Inquired of the Information Security Director regarding audit logging to determine that log data was immutable and could not be modified. | No exceptions noted. |
| | | | Inspected the audit logging dashboard and configurations to determine that log data was immutable and could not be modified. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The connection between the logging server and the production environment is encrypted. | Inspected the encryption configuration for data in transit between the production environment and the logging server to determine that the connection between the logging server and the production environment was encrypted. | No exceptions noted. |
| OPS-15 | The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. | Application audit logging configurations are in place to log user activity and system events. | Inspected the application audit logging configurations to determine that application audit logging configurations were in place to log user activity and system events. | No exceptions noted. |
| | Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication. | Application audit logs are maintained and available for review when needed. | Inquired of the Information Security Director regarding the application audit logs to determine that application audit logs were maintained and available for review when needed. | No exceptions noted. |
| | | | Inspected an example application audit log extract to determine that application audit logs were maintained and available for review when needed. | No exceptions noted. |
| OPS-16 | Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorized users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03). | Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | Inspected the information security and the incident response policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | A role-based access control system was utilized to restrict write access to log files to the administrator group members. | Inspected the network administrator group listing to determine that a role-based access control system was utilized to restrict write access to log files to the administrator group members. | No exceptions noted. |
| | | System changes are authorized and approved by management prior to implementation. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were authorized and approved by management prior to implementation. | No exceptions noted. |
| OPS-17 | The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action. | Logs from information systems are aggregated and secured to a central repository. | Inspected the dashboard for log file storage and analysis to determine that logs from information systems were aggregated and secured to a central repository. | No exceptions noted. |
| | | The logging system is configured to automatically alert authorized personnel in the event an anomalous logging event or irregularity is detected. | Inspected the audit logging alert configurations and an example alert to determine that the logging system was configured to automatically alert authorized personnel in the event an anomalous logging event or irregularity was detected. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-18 | Guidelines and instructions with technical and organizational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects:<br>• Regular identification of vulnerabilities<br>• Assessment of the severity of identified vulnerabilities<br>• Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines<br>• Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment. | No exceptions noted. |
| | | SOPs are reviewed by management on an annual basis. | Inspected the entity's SOPs with the revision history to determine that SOPs were reviewed by management on an annual basis. | No exceptions noted. |
| | | Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment. | Inspected the vulnerability management process policies and procedures to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment. | No exceptions noted. |
| | | Vulnerability scans and penetration tests are performed and remedial actions are taken where necessary. | Inspected the completed vulnerability scan results for a sample of quarters and completed penetration test results to determine that vulnerability scans and penetration tests were performed and remedial actions were taken where necessary. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to:<br>• Rebuilding systems<br>• Updating software<br>• Installing patches<br>• Removing unauthorized access<br>• Changing configurations | Inspected the information security, incident response, and change management policies and procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to:<br>• Rebuilding systems<br>• Updating software<br>• Installing patches<br>• Removing unauthorized access<br>• Changing configurations | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-19 | The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis.<br><br>The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria.<br><br>For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation. | Vulnerability scans and penetration tests are performed and remedial actions are taken where necessary.<br><br>Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. | Inspected the completed vulnerability scan results for a sample of quarters and completed penetration test results to determine that vulnerability scans and penetration tests were performed and remedial actions were taken where necessary.<br><br>Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| OPS-20 | The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness.<br><br>Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness. | The incident response policies procedures are reviewed at least on an annual basis for effectiveness. | Inspected the revision history of the incident response policies and procedures to determine that the incident response policies and procedures were reviewed at least on an annual basis for effectiveness. | No exceptions noted. |
| OPS-21 | The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements. | Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| | As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken. | Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. | Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The actions taken to address identified security incidents are documented and communicated to affected parties. | Inspected the supporting incident tickets for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties. | No exceptions noted. |
| | | Resolution of incidents are documented within the ticket and communicated to affected users. | Inspected the supporting incident tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users. | No exceptions noted. |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. | Inquired of the Information Security Director regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | Testing of the control activity disclosed that there were no critical incidents during the review period. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The entity communicates major system events that can impact the security or availability of their services through the publicly accessible company web portal. | Inquired of the Information Security Director regarding incident communication to customers to determine that the entity communicated major system events that could impact the security or availability of their services through the publicly accessible company web portal. | No exceptions noted. |
| | | | Inspected the company website to determine that the entity communicated major system events that could impact the security or availability of their services through the publicly accessible company web portal. | No exceptions noted. |
| OPS-22 | System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment. | Inspected the vulnerability management process policies and procedures to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Vulnerability scans and penetration tests are performed and remedial actions are taken where necessary. | Inspected the completed vulnerability scan results for a sample of quarters and completed penetration test results to determine that vulnerability scans and penetration tests were performed and remedial actions were taken where necessary. | No exceptions noted. |
| OPS-23 | System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented. | System hardening policies and procedures are in place. | Inspected the system hardening procedures to determine that system hardening policies and procedures were in place. | No exceptions noted. |
| | | Organizationally owned systems are configured to management approved standards or requirements prior to being commissioned. | Inspected the information security policies and procedures to determine that all organizationally owned systems were configured to management approved standards or requirements prior to being commissioned. | No exceptions noted. |
| | If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained. | Installation of applications on organizationally owned mobile devices is restricted to approved application stores and jailbreaking, rooting, and side-loading of applications is prohibited. | Inquired of the Information Security Director to determine that installation of applications on organizationally owned mobile devices was restricted to approved application stores, and that jailbreaking, rooting, and side-loading of applications was prohibited. | No exceptions noted. |

| CONTROL DOMAIN: OPERATIONS (OPS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the warning message for an example attempt to download application to determine that installation of applications on organizationally owned mobile devices was restricted to approved application stores, and that jailbreaking, rooting, and side-loading of applications was prohibited. | No exceptions noted. |
| OPS-24 | Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data. | Customer data is segregated from other data. | Inspected the dataflow diagrams and cloud environments to determine that customer data was segregated from other data. | No exceptions noted. |
| | | The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. | Inspected the network diagram and VPC configurations to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel. | No exceptions noted. |
| | | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-01 | A role and rights concept based on the business and security requirements of the Cloud Service Provider as well as a policy for managing user accounts and access rights for internal and external employees of the Cloud Service Provider and system components that have a role in automated authorization processes of the Cloud Service Provider are documented, communicated, and made available according to SP-01:<br>• Assignment of unique usernames<br>• Granting and modifying user accounts and access rights based on the "least-privilege- principle" and the "need-to-know" principle<br>• Segregation of duties between operational and monitoring functions ("Segregation of Duties")<br>• Segregation of duties between managing, approving and assigning user accounts and access rights<br><br>**Continues on the next page.* | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment. | No exceptions noted. |
| | | SOPs are reviewed by management on an annual basis. | Inspected the entity's SOPs with the revision history to determine that SOPs were reviewed by management on an annual basis. | No exceptions noted. |
| | | Privileged access to sensitive resources is restricted to authorized personnel. | Inquired of the Information Security Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the listings of privileged users to the in-scope systems to determine that privileged access to sensitive resources was restricted to authorized personnel. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Approval by authorized individual(s) or system(s) for granting or modifying user accounts and access rights before data of the cloud customer or system components used to provision the cloud service can be accessed<br>• Regular review of assigned user accounts and access rights<br>• Blocking and removing access accounts in the event of inactivity<br>• Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility<br>• Two-factor or multi-factor authentication for users with privileged access<br>• Requirements for the approval and documentation of the management of user accounts and access rights | | | |
| | **Internal Network - Okta** | | | |
| | | Network user access is restricted via role-based security privileges defined within the access control system. | Inspected the network user listing and access roles to determine that network user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Network administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the network to determine that network administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the network administrator listing and access roles to determine that network administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Networks are configured to enforce password requirements that include:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | Inspected the network password settings to determine that networks were configured to enforce password requirements that included:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | No exceptions noted. |
| | **Operating Systems - Linux** | | | |
| | | Operating system user access is restricted via role-based security privileges defined within the access control system. | Inspected the operating system user listing and access roles to determine that operating system user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Operating system administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding the administrative access to the operating system to determine that operating system administrative access was restricted to authorized personnel. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the operating system administrator listing and access roles to determine that operating system administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Operating system users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that operating system users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |
| | **Database - PostgreSQL** | | | |
| | | Databases user access is restricted via role-based security privileges defined within the access control system. | Inspected the databases user listing and access roles to determine that databases user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Databases administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the databases to determine that databases administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the databases administrator listing and access roles to determine that databases administrative access was restricted to authorized personnel. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Databases users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that databases users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |
| | **Application - Helix Platform** | | | |
| | | Application user access is restricted via role-based security privileges defined within the access control system. | Inspected the application user listing and access roles to determine that application user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Application administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the application to determine that application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the application administrator listing and access roles to determine that application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Application users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that application users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | End-user access to the in-scope application requires a unique username and password combination and the authentication requirements can be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | Inquired of the Information Security Director regarding application authentication to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | | | Observed a user authenticate to the in-scope application to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | **VPN Connection - Cisco AnyConnect** | | | |
| | | VPN user access is restricted via role-based security privileges defined within the access control system. | Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | The ability to administer VPN access is restricted to user accounts accessible by authorized personnel. | Inquired of the Information Security Director regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| | | VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system. | Inquired of the Information Security Director regarding VPN Access to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |
| | | | Observed a user authenticate to the VPN access to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |
| | | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inquired of the Information Security Director regarding new hire access to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | | Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired of the Information Security Director regarding logical access removal to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |
| | | | Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-02 | Specified procedures for granting and modifying user accounts and access rights for internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorization processes of the Cloud Service Provider ensure compliance with the role and rights concept as well as the policy for managing user accounts and access rights. | Privileged access to sensitive resources is restricted to authorized personnel. | Inquired of the Information Security Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the listings of privileged users to the in-scope systems to determine that privileged access to sensitive resources was restricted to authorized personnel. | No exceptions noted. |
| | | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |
| | | | Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inquired of the Information Security Director regarding new hire access to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | | Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired of the Information Security Director regarding logical access removal to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | SOPs are reviewed by management on an annual basis. | Inspected the entity's SOPs with the revision history to determine that SOPs were reviewed by management on an annual basis. | No exceptions noted. |
| IDM-03 | User accounts of internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorization processes of the Cloud Service Provider are automatically locked if they have not been used for a period of two months. Approval from authorized personnel or system components are required to unlock these accounts.<br><br>Locked user accounts are automatically revoked after six months. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated. | Network user accounts are disabled after 90 days of inactivity. | Inspected the inactivity configurations and the completed user access review to determine that network user accounts were disabled after 90 days of inactivity. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-04 | Access rights are promptly revoked if the job responsibilities of the Cloud Service Provider's internal or external staff or the tasks of system components involved in the Cloud Service Provider's automated authorization processes change. Privileged access rights are adjusted or revoked within 48 hours after the change taking effect. All other access rights are adjusted or revoked within 14 days. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated. | Network user accounts are disabled after 90 days of inactivity. | Inspected the completed user account review to determine that network user accounts were disabled after 90 days of inactivity. | No exceptions noted. |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired of the Information Security Director regarding logical access removal to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | | Inspected the termination procedures, user access listings for the in-scope systems and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-05 | Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorization processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorized persons from the Cloud Service Provider's organizational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights. | Logical access is reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts. | Inquired of the Information Security Director regarding logical access reviews to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.<br><br>Inspected the completed logical access review for a sample of quarters to determine that logical access was reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-06 | Privileged access rights for internal and external employees as well as technical users of the Cloud Service Provider are assigned and changed in accordance with the policy for managing user accounts and access rights (cf. IDM-01) or a separate specific policy.<br><br>Privileged access rights are personalized, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ("need-to-know principle"). Technical users are assigned to internal or external employees of the Cloud Service Provider.<br><br>Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases. The logged information is automatically monitored for defined events that may indicate misuse. When such an event is identified, the responsible personnel are automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04. | Privileged access to sensitive resources is restricted to authorized personnel.<br><br>Logs from information systems are aggregated and secured to a central repository.<br><br>The logging system is configured to automatically alert authorized personnel in the event an anomalous logging event or irregularity is detected.<br><br>Sanction policies, which include suspension and termination, are in place for employee misconduct or violation of the entity's policies and procedures. | Inquired of the Information Security Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.<br><br>Inspected the listings of privileged users to the in-scope systems to determine that privileged access to sensitive resources was restricted to authorized personnel.<br><br>Inspected the dashboard for log file storage and analysis to determine that logs from information systems were aggregated and secured to a central repository.<br><br>Inspected the audit logging alert configurations and an example alert to determine that the logging system was configured to automatically alert authorized personnel in the event an anomalous logging event or irregularity was detected.<br><br>Inspected the sanction policies and procedures to determine that sanction policies, which include suspension and termination, were in place for employee misconduct or violation of the entity's policies and procedures. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Policies and procedures are in place for malware detection, prevention, and response processes. | Inspected the antivirus policies and procedures to determine that policies and procedures were in place for malware detection, prevention, and response processes. | No exceptions noted. |
| IDM-07 | The cloud customer is informed by the Cloud Service Provider whenever internal or external employees of the Cloud Service Provider read or write to the cloud customer's data processed, stored or transmitted in the cloud service or have accessed it without the prior consent of the cloud customer. The Information is provided whenever data of the cloud customer is/was not encrypted, the encryption is/was disabled for access or the contractual agreements do not explicitly exclude such information. The information contains the cause, time, duration, type and scope of the access. The information is sufficiently detailed to enable subject matter experts of the cloud customer to assess the risks of the access. The information is provided in accordance with the contractual agreements, or within 72 hours after the access. | Not applicable. Cloud customer data is not directly accessible to the entity's employees. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-08 | The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud provider and system components that are involved in automated authorization processes of the cloud provider is done in an orderly manner that ensures the confidentiality of the information. If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible:<br>• Users can initially create the password themselves or must change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days<br>• When creating passwords, compliance with the password specifications (cf. IDM-12) is enforced as far as technically possible<br>• The user is informed about changing or resetting the password<br>• The server-side storage takes place using cryptographically strong hash functions<br><br>*Continues on the next page.* | User authentication and access control policies and procedures are in place to guide personnel on the entity's authentication requirements. | Inspected the access control policies and procedures to determine that user authentication and access control policies and procedures were in place to guide personnel on the entity's authentication requirements. | No exceptions noted. |
| | | Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. | Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. | No exceptions noted. |
| | | Stored passwords are encrypted. | Inspected the encryption configurations for data at rest to determine that stored passwords were encrypted. | No exceptions noted. |
| | | Critical data is stored in encrypted format using software supporting the AES256. | Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES256. | No exceptions noted. |
| | | Encryption keys are protected during generation, storage, use, and destruction. | Inspected the encryption policies and procedures to determine that encryption keys were protected during generation, storage, use, and destruction. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented | End-user access to the in-scope application requires a unique username and password combination and the authentication requirements can be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | Inquired of the Information Security Director regarding application authentication to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | | | Observed a user authenticate to the in-scope application to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Documented confidential policies and procedures are in place that include the following:<br>• Defining, identifying, and designating information as confidential<br>• Storing confidential information<br>• Protecting confidential information from erasure or destruction<br>• Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed | Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place that included:<br>• Defining, identifying, and designating information as confidential<br>• Storing confidential information<br>• Protecting confidential information from erasure or destruction<br>• Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| IDM-09 | System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service, authenticate users of the Cloud Service Provider's internal and external employees as well as system components that are involved in the Cloud Service Provider's automated authorizations processes. Access to the production environment requires two-factor or multi-factor authentication. Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the Guideline for Key Management (cf. CRY-01). The password requirements are derived from a risk assessment and documented, communicated and provided in a password policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible. | User authentication and access control policies and procedures are in place to guide personnel on the entity's authentication requirements. | Inspected the access control policies and procedures to determine that user authentication and access control policies and procedures were in place to guide personnel on the entity's authentication requirements. | No exceptions noted. |
| | | Privileged access to sensitive resources is restricted to authorized personnel. | Inquired of the Information Security Director regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel. | No exceptions noted. |
| | | | Inspected the listings of privileged users to the in-scope systems to determine that privileged access to sensitive resources was restricted to authorized personnel. | No exceptions noted. |
| | | A single sign-on and identity management platform supporting multi-factor authentication is utilized as the role-based access control system for cloud-based applications. | Inspected the authentication configurations to determine that a single sign-on and identity management platform supporting multi-factor authentication was utilized as the role-based access control system for cloud-based applications. | No exceptions noted. |
| | | Traffic to and from the web-based application and mobile applications that utilize the API are secured using encryption methods to ensure message confidentiality and integrity. | Inspected the encryption methods and configurations to determine that traffic to and from the web-based application and mobile applications that utilize the API were secured using encryption methods to ensure message confidentiality and integrity. | No exceptions noted. |

| CONTROL DOMAIN: IDENTITY AND ACCESS MANAGEMENT (IDM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | End-user access to the in-scope application requires a unique username and password combination and the authentication requirements can be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | Inquired of the Information Security Director regarding application authentication to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | | | Observed a user authenticate to the in-scope application to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment. | No exceptions noted. |
| | | SOPs are reviewed by management on an annual basis. | Inspected the entity's SOPs with the revision history to determine that SOPs were reviewed by management on an annual basis. | No exceptions noted. |

| CONTROL DOMAIN: CRYPTOGRAPHY AND KEY MANAGEMENT (CRY) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CRY-01 | Policies and instructions with technical and organizational safeguards for encryption procedures and key management are documented, communicated and provided according to SP-01, in which the following aspects are described:<br>• Usage of strong encryption procedures and secure network protocols that correspond to the state-of-the-art<br>• Risk-based provisions for the use of encryption which are aligned with the data classification schemes and consider the communication channel, type, strength and quality of the encryption<br>• Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys<br>• Consideration of relevant legal and regulatory obligations and requirements | SOPs are in place that define system operation requirements mandatory for maintaining the cloud service environment.<br><br>SOPs are reviewed by management on an annual basis.<br><br>The organization has developed and implemented policies and procedures for cryptographic requirements. | Inspected the entity's SOPs to determine that SOPs were in place that defined system operation requirements mandatory for maintaining the cloud service environment.<br><br>Inspected the entity's SOPs with the revision history to determine that SOPs were reviewed by management on an annual basis.<br><br>Inspected the encryption policies and procedures to determine that the organization had developed and implemented policies and procedures for cryptographic requirements. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |
| CRY-02 | The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of data of cloud customers over public networks. | The organization has developed and implemented policies and procedures for cryptographic requirements. | Inspected the encryption policies and procedures to determine that the organization had developed and implemented policies and procedures for cryptographic requirements. | No exceptions noted. |

| CONTROL DOMAIN: CRYPTOGRAPHY AND KEY MANAGEMENT (CRY) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | End-user access to the in-scope application requires a unique username and password combination and the authentication requirements can be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | Inquired of the Information Security Director regarding application authentication to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | | | Observed a user authenticate to the in-scope application to determine that end-user access to the in-scope application required a unique username and password combination and the authentication requirements could be enhanced by the cloud service customer with the inclusion of multi-factor authentication. | No exceptions noted. |
| | | Backup media is stored in an encrypted format. | Inspected the backup encryption configurations to determine that backup media was stored in an encrypted format. | No exceptions noted. |
| | | Transmission of digital output beyond the boundary of the system is encrypted. | Inspected the encryption configurations for data in transit to determine that transmission of digital output beyond the boundary of the system was encrypted. | No exceptions noted. |

| CONTROL DOMAIN: CRYPTOGRAPHY AND KEY MANAGEMENT (CRY) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CRY-03 | The Cloud Service Provider has established procedures and technical safeguards to encrypt cloud customers' data during storage. The private keys used for encryption are known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements. Exceptions follow a specified procedure. The procedures for the use of private keys, including any exceptions, must be contractually agreed with the cloud customer. | The organization has developed and implemented policies and procedures for key management. | Inspected the encryption policies and procedures to determine that the organization had developed and implemented policies and procedures for key management. | No exceptions noted. |
| | | Access to encryption keys is restricted to authorized personnel only. | Inspected user access privileges defined in the network to determine that access to encryption keys was restricted to authorized personnel only. | No exceptions noted. |
| | | Backup media is stored in an encrypted format. | Inspected the backup encryption configurations to determine that backup media was stored in an encrypted format. | No exceptions noted. |

| CONTROL DOMAIN: CRYPTOGRAPHY AND KEY MANAGEMENT (CRY) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| CRY-04 | Procedures and technical safeguards for secure key management in the area of responsibility of the Cloud Service Provider include at least the following aspects:<br>• Generation of keys for different cryptographic systems and applications<br>• Issuing and obtaining public-key certificates<br>• Provisioning and activation of the keys<br>• Secure storage of keys (separation of key management system from application and middleware level) including description of how authorized users get access<br>• Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realized<br>• Handling of compromised keys.<br>• Withdrawal and deletion of keys<br>• If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately | The organization has developed and implemented policies and procedures for key management.<br><br>Access to encryption keys is restricted to authorized personnel only. | Inspected the encryption policies and procedures to determine that the organization had developed and implemented policies and procedures for key management.<br><br>Inspected the user access privileges defined in the network to determine that access to encryption keys was restricted to authorized personnel only. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: COMMUNICATION SECURITY (COS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COS-01 | Based on the results of a risk analysis carried out according to OIS-06, the Cloud Service Provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial- of-Service (DDoS) attacks. Data from corresponding technical protection measures implemented is fed into a comprehensive SIEM (Security Information and Event Management) system, so that (counter) measures regarding correlating events can be initiated. The safeguards are documented, communicated, and provided in accordance with SP-01. | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | The monitoring software is configured to alert IT personnel when thresholds have been exceeded. | Inspected the monitoring tool configurations and an example alert to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded. | No exceptions noted. |
| | | Network traffic to information systems hosting customer data is filtered to allow connections based on pre-defined criteria. | Inspected the routing table, VLAN definitions for the virtual distributed switch and compared to the firewall rulesets for the production environment to determine that network traffic to information systems hosting customer data was filtered to allow connections based on pre-defined criteria. | No exceptions noted. |

| CONTROL DOMAIN: COMMUNICATION SECURITY (COS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COS-02 | Specific security requirements are designed, published and provided for establishing connections within the Cloud Service Provider's network. The security requirements define for the Cloud Service Provider's area of responsibility:<br>• In which cases the security zones are to be separated and in which cases cloud customers are to be logically or physically segregated<br>• Which communication relationships and which network and application protocols are permitted in each case<br>• How the data traffic for administration and monitoring is segregated from each on network level<br>• Which internal, cross-location communication is permitted<br>• Which cross-network communication is allowed | Separate development, testing, and production environments are maintained. | Inspected the network diagrams and cloud environment to determine that separate development, testing, and production environments were maintained. | No exceptions noted. |
| | | Customer data is segregated from other data. | Inspected the dataflow diagrams and cloud environments to determine that customer data was segregated from other data. | No exceptions noted. |
| | | Critical infrastructure components (e.g., routers, databases, data storage) are reviewed for criticality and configured with a minimum level of redundancy that includes:<br>• Stateful failover of high-availability firewalls<br>• Near real-time cross-site replication of databases<br>• Near real-time cross-site replication of data storage | Inspected the infrastructure failover configurations to determine that critical infrastructure components (e.g., routers, databases, data storage) were reviewed for criticality and configured with a minimum level of redundancy that included:<br>• Stateful failover of high-availability firewalls<br>• Near real-time cross-site replication of databases<br>• Near real-time cross-site replication of data storage | No exceptions noted. |
| | | Network traffic to information systems hosting customer data is filtered to allow connections based on pre-defined criteria. | Inspected the routing table, VLAN definitions for the virtual distributed switch and compared to the firewall rulesets for the production environment to determine that network traffic to information systems hosting customer data was filtered to allow connections based on pre-defined criteria. | No exceptions noted. |

| CONTROL DOMAIN: COMMUNICATION SECURITY (COS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COS-03 | A distinction is made between trusted and untrusted networks. Based on a risk assessment, these are separated into different security zones for internal and external network areas (and DMZ, if applicable). Physical and virtualized network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements.<br><br>The entirety of the conception and configuration undertaken to monitor the connections mentioned is assessed in a risk-oriented manner, at least annually, regarding the resulting security requirements.<br><br>Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).<br><br>At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure. | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |
| | | Network traffic to information systems hosting customer data is filtered to allow connections based on pre-defined criteria. | Inspected the routing table, VLAN definitions for the virtual distributed switch and compared to the firewall rulesets for the production environment to determine that network traffic to information systems hosting customer data was filtered to allow connections based on pre-defined criteria. | No exceptions noted. |
| | | Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed. | Inspected the ISPMS Management Review to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed. | No exceptions noted. |
| | | Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions. | No exceptions noted. |

| CONTROL DOMAIN: COMMUNICATION SECURITY (COS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | All in-scope services, protocols and ports are reviewed by management on at least an annual basis. | Inspected the firewall ruleset for the production environment to determine that all in-scope services, protocols and ports were reviewed by management on at least an annual basis. | No exceptions noted. |
| COS-04 | Each network perimeter is controlled by security gateways. The system access authorization for cross-network access is based on a security assessment based on the requirements of the cloud customers. | The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. | Inspected the network diagram and VPC configurations to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel. | No exceptions noted. |
| COS-05 | There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication (cf. IDM-09). Networks used by the Cloud Service Provider to migrate or create virtual machines are also physically or logically separated from other networks. | Separate development, testing, and production environments are maintained. | Inspected the network diagrams and cloud environment to determine that separate development, testing, and production environments were maintained. | No exceptions noted. |
| | | Customer data is segregated from other data. | Inspected the production databases and dataflow diagrams to determine that customer data was segregated from other data. | No exceptions noted. |
| | | Access to the network administrator dashboard is restricted to authorized personnel and requires the use of multi-factor authentication. | Inquired of the Information Security Director regarding administrative access to determine that access to the network administrator dashboard was restricted to authorized personnel and required the use of multi-factor authentication. | No exceptions noted. |

| CONTROL DOMAIN: COMMUNICATION SECURITY (COS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the network administrator user listing and the network authentication configurations to determine that access to the network administrator dashboard was restricted to authorized personnel and required the use of multi-factor authentication. | No exceptions noted. |
| COS-06 | Data traffic of cloud customers in jointly used network environments is segregated on network level according to a documented concept to ensure the confidentiality and integrity of the data transmitted. | Separate development, testing, and production environments are maintained. | Inspected the network diagrams and cloud environment to determine that separate development, testing, and production environments were maintained. | No exceptions noted. |
| | | Customer data is segregated from other data in accordance with the documented system data flow and cloud infrastructure diagrams. | Inspected the production databases and network diagrams to determine that customer data was segregated from other data in accordance with the documented system data flow and cloud infrastructure diagrams. | No exceptions noted. |
| COS-07 | The documentation of the logical structure of the network used to provision or operate the Cloud Service, is traceable and up to date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions in accordance with contractual obligations. The documentation shows how the subnets are allocated and how the network is zoned and segmented. In addition, the geographical locations in which the cloud customers' data is stored are indicated. | Organizational and information security policies and procedures are documented and made available to employee's through the entity's shared drive. | Inspected the information security policies and procedures and the entity's shared drive to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's shared drive. | No exceptions noted. |
| | | The network diagram is reviewed on an annual basis and updates are made when needed. | Inspected the network diagram to determine that the network diagram was reviewed on an annual basis and updates were made when needed. | No exceptions noted. |

| CONTROL DOMAIN: COMMUNICATION SECURITY (COS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Geographic redundancy is built into the infrastructure through the utilization of third-party data centers in geographically dispersed, disaster-neutral locations. | Inquired of the Information Security Director regarding geographic redundancy to determine that geographic redundancy was built into the infrastructure through the utilization of third-party data centers in geographically dispersed, disaster-neutral locations. | No exceptions noted. |
| | | | Inspected the network diagram and business continuity plan to determine that geographic redundancy was built into the infrastructure through the utilization of third-party data centers in geographically dispersed, disaster-neutral locations. | No exceptions noted. |
| COS-08 | Policies and instructions with technical and organizational safeguards in order to protect the transmission of data against unauthorized interception, manipulation, copying, modification, redirection, or destruction are documented, communicated and provided according to SP-01. The policy and instructions establish a reference to the classification of information (cf. AM-06). | The organization has developed and implemented policies and procedures for key management. | Inspected the encryption policies and procedures to determine that the organization had developed and implemented policies and procedures for key management. | No exceptions noted. |
| | | Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. | Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. | No exceptions noted. |

| CONTROL DOMAIN: PORTABILITY AND INTEROPERABILITY (PI) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PI-01 | The cloud service can be accessed by other cloud services or IT systems of cloud customers through documented inbound and outbound interfaces. Further, the interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. | Authorization for connecting to the API is mandatory, which is enabled using proprietary solutions as well as open standards for authorization such as OAuth 2.0. | Inquired of the Information Security Director regarding API authentication to determine that authorization for connecting to the API was mandatory, which was enabled using proprietary solutions as well as open standards for authorization such as OAuth 2.0. | No exceptions noted. |
| | Communication takes place through standardized communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks is encrypted according to CRY-02. | | Observed a user connect the in-scope API to determine that authorization for connecting to the API was mandatory, which was enabled using proprietary solutions as well as open standards for authorization such as OAuth 2.0. | No exceptions noted. |
| | The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces. The information is maintained in such a way that it is applicable for the cloud service's version which is intended for productive use. | Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. | Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. | No exceptions noted. |
| | | API documentation for the organization’s application is available on a public-facing website. | Inspected the organization’s front-facing resource center and technical documentation to determine that API documentation for the organization’s application was available on a public-facing website. | No exceptions noted. |

| CONTROL DOMAIN: PORTABILITY AND INTEROPERABILITY (PI) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PI-02 | In contractual agreements, the following aspects are defined with regard to the termination of the contractual relationship, insofar as these are applicable to the cloud service:<br>• Type, scope and format of the data the Cloud Service Provider provides to the cloud customer<br>• Definition of the timeframe, within which the Cloud Service Provider makes the data available to the cloud customer<br>• Definition of the point in time as of which the Cloud Service Provider makes the data inaccessible to the cloud customer and deletes these<br>• The cloud customers' responsibilities and obligations to cooperate for the provision of the data<br>• The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the Cloud Service Provider as well as legal and regulatory requirements | Customers are required to adhere to the termination requirements provided in the master service agreement. | Inquired of the Information Security Director regarding customer commitments to determine that customers were required to adhere to the termination requirements provided in the master service agreement. | No exceptions noted. |
| | | | Inspected the executed agreement for a sample of customers to determine that customers were required to adhere to the termination requirements provided in the master service agreement. | No exceptions noted. |
| | | Customer content is released to the customer upon termination of service contract, if requested. | Inquired of the Information Security Director regarding customer commitments to determine that customer content was release to the customer upon termination. | No exceptions noted. |
| | | | Inspected the data processing addendum template to determine that customer content was released to the customer upon termination of service contract, if requested. | No exceptions noted. |
| | | Customer data is retained for 90 days after the respective contract is terminated. After this threshold is exceeded, the data is removed from the system. | Inquired of the Information Security Director regarding customer data commitments to determine that customer data was retained for 90 days after the respective contract was terminated, and that after this threshold was exceeded, the data was removed from the system. | No exceptions noted. |

| CONTROL DOMAIN: PORTABILITY AND INTEROPERABILITY (PI) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the data classification, handling and disposal policies and procedures to determine that customer data was retained for 90 days after the respective contract was terminated, and that after this threshold was exceeded, the data was removed from the system. | No exceptions noted. |
| PI-03 | The Cloud Service Provider's procedures for deleting the cloud customers' data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02).<br><br>The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups.<br><br>The deletion procedures prevent recovery by forensic means. | The removal of all cloud customer data, inclusive of all data within the cloud customer's environment, any related cloud customer metadata, and any stored backup data pertaining to the cloud customer upon termination of services is defined within the master service agreement. | Inspected the executed agreement for a sample of customers to determine that the removal of all cloud customer data, inclusive of all data within the cloud customer's environment, any related cloud customer metadata, and any stored backup data pertaining to the cloud customer upon termination of services was defined within the master service agreement. | No exceptions noted. |
| | Disk sanitizers are utilized to securely remove customer data on storage medium from the production environment. | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | Not applicable. | Not applicable. |
| | | Automated processes are implemented to remove all customer data from the production environment. | Inquired of the Information Security Director regarding customer data removal to determine that automated processes were implemented to remove all customer data from the production environment. | No exceptions noted. |

| CONTROL DOMAIN: PORTABILITY AND INTEROPERABILITY (PI) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | | Inspected the data classification, handling and disposal policies and procedures and retention schedule to determine that automated processes were implemented to remove all customer data from the production environment. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| DEV-01 | Policies and instructions with technical and organizational measures for the secure development of the cloud service are documented, communicated and provided in accordance with SP-01. | Documented change control policies and procedures are in place to guide personnel in the change management process. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process. | No exceptions noted. |
| | The policies and instructions contain guidelines for the entire life cycle of the cloud service and are based on recognized standards and methods with regard to the following aspects:<br>• Security in Software Development (Requirements, Design, Implementation, Testing and Verification)<br>• Security in software deployment (including continuous delivery)<br>• Security in operation (reaction to identified faults and vulnerabilities) | The change management process has defined the following roles and assignments:<br>• Authorization of change requests- Authorized personnel from the Customer<br>• Development - Trained SaaS Personnel<br>• Testing - Trained SaaS Personnel<br>• Implementation - Trained SaaS Personnel | Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments:<br>• Authorization of change requests- Authorized personnel from the Customer<br>• Development - Trained SaaS Personnel<br>• Testing - Trained SaaS Personnel<br>• Implementation - Trained SaaS Personnel | No exceptions noted. |
| | | The entity establishes patch and change management policies and procedures to address equipment maintenance for ensuring security and availability. | Inspected the change management policies and procedures to determine that the entity established patch and change management policies and procedures to address equipment maintenance for ensuring security and availability. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| DEV-02 | In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the Cloud Service Provider and the outsourced development contractor:<br>• Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognized standards and methods<br>• Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements<br>• Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities | Not applicable. The entity did not utilize external developers / contractors for change management, release, and testing. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| DEV-03 | Policies and instructions with technical and organizational safeguards for change management of system components of the cloud service within the scope of software deployment are documented, communicated, and provided according to SP-01 with regard to the following aspects:<br>• Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorized personnel or system components<br>• Requirements for the performance and documentation of tests<br>• Requirements for segregation of duties during development, testing and release of changes<br><br>**Continues on the next page.* | Documented change control policies and procedures are in place to guide personnel in the change management process. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process. | No exceptions noted. |
| | | The change management process has defined the following roles and assignments:<br>• Authorization of change requests- Authorized personnel from the Customer<br>• Development - Trained SaaS Personnel<br>• Testing - Trained SaaS Personnel<br>• Implementation - Trained SaaS Personnel | Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments:<br>• Authorization of change requests- Authorized personnel from the Customer<br>• Development - Trained SaaS Personnel<br>• Testing - Trained SaaS Personnel<br>• Implementation - Trained SaaS Personnel | No exceptions noted. |
| | | The entity establishes patch and change management policies and procedures to address equipment maintenance for ensuring security and availability. | Inspected the change management policies and procedures to determine that the entity established patch and change management policies and procedures to address equipment maintenance for ensuring security and availability. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements<br>• Requirements for the documentation of changes in system, operational and user documentation<br>• Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes | Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation. | No exceptions noted. |
| DEV-04 | The Cloud Service Provider provides a training program for regular, target group-oriented security training and awareness for internal and external employees on standards and methods of secure software development and provision as well as on how to use the tools used for this purpose. The program is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used. | Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | Inspected the signed employee code of conduct acknowledgement, and information security and awareness training completion form for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | Inspected the signed employee code of conduct acknowledgement, and information security and awareness training completion form a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis. | No exceptions noted. |
| DEV-05 | In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment with regard to potential effects on the system components concerned and are categorized and prioritized accordingly. | The risk factors for change implementation are calculated and evaluated as a component of the change management process. | Inspected the change management policies and procedures to determined that the risk factors for change implementation were calculated and evaluated as a component of the change management process. | No exceptions noted. |
| | | Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment. | Inspected the risk assessment policies and procedures and the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| DEV-06 | Changes to the cloud service are subject to appropriate testing during software development and deployment.<br><br>The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the Cloud Service Provider or by automated test procedures that comply with the state-of-the-art. Cloud customers are involved into the tests in accordance with the contractual requirements.<br><br>The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated. | System changes are tested prior to implementation and types of testing performed depend on the nature of the change.<br><br>Management follows a methodical process to identify assets, associated threats and vulnerabilities, and quantifies the probability, and harm that may be inflicted. Vulnerabilities are to be addressed in a timely manner and prioritized based on severity. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.<br><br>Inspected the change management policies and procedures, the risk assessment policies and procedures, and the completed risk assessment to determine that management followed a methodical process to identify assets, associated threats and vulnerabilities, and quantified the probability, and harm that could be inflicted, and that vulnerabilities were to be addressed in a timely manner and prioritized based on severity. | No exceptions noted.<br><br>No exceptions noted. |
| DEV-07 | System components and tools for source code management and software deployment that are used to make changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IDM-01 and authorization mechanisms. They must be configured in such a way that all changes are logged and can therefore be traced back to the individuals or system components executing them. | Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. | Inspected the change control software configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Access to implement changes in the production environment is restricted to authorized IT personnel. | Inquired of the Information Security Director regarding the users with access to deploy changes to determine that access to implement changes in the production environment was restricted to authorized IT personnel. | No exceptions noted. |
| | | | Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel. | No exceptions noted. |
| | | Source code changes are logged, reviewed, tested, and approved. | Inspected the change ticket for a sample of application changes to determine that source code changes were logged, reviewed, tested, and approved. | No exceptions noted. |
| DEV-08 | Version control procedures are set up to track dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities. | Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation. | No exceptions noted. |

| CONTROL DOMAIN: PROCUREMENT, DEVELOPENT AND MODIFICATION OF INFORMATION SYSTEMS (DEV) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| DEV-09 | Authorized personnel or system components of the Cloud Service Provider approve changes to the cloud service based on defined criteria (e.g., test results and required approvals) before these are made available to the cloud customers in the production environment.<br><br>Cloud customers are involved in the release according to contractual requirements. | System changes are tested prior to implementation and types of testing performed depend on the nature of the change. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change. | No exceptions noted. |
| | | System changes are authorized and approved by management prior to implementation. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were authorized and approved by management prior to implementation. | No exceptions noted. |
| | | Not applicable. Part of the criterion is not applicable to the system in scope, as customers are not involved in the change management process and user acceptance testing is not performed per the entity's business model. | Not applicable. | Not applicable. |
| DEV-10 | Production environments are physically or logically separated from test or development environments to prevent unauthorized access to cloud customer data, the spread of malware, or changes to system components. Data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality. | Separate development, testing, and production environments are maintained. | Inspected the network diagrams and cloud environment to determine that separate development, testing, and production environments were maintained. | No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SSO-01 | Policies and instructions for controlling and monitoring third-parties (e.g. service providers or suppliers) whose services contribute to the provision of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects:<br>• Requirements for the assessment of risks resulting from the procurement of third-party services<br>• Requirements for the classification of third-parties based on the risk assessment by the Cloud Service Provider and the determination of whether the third-party is a subcontractor (cf Supplementary Information)<br>• Information security requirements for the processing, storage or transmission of information by third-parties based on recognized industry standards<br>• Information security awareness and training requirements for staff<br><br>**Continues on the next page.* | Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. | Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances. | No exceptions noted. |
| | | Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. | Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process. | No exceptions noted. |
| | | Identified third-party risks are rated using a risk evaluation process and ratings are approved by management. | Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that identified third-party risks were rated using a risk evaluation process and ratings are approved by management. | No exceptions noted. |
| | | A third-party agreement outlines and communicates the terms, conditions, and responsibilities of third-parties. | Inspected the executed third-party agreement for a sample third-parties to determine that a third-party agreement outlined and communicated the terms, conditions, and responsibilities of third-parties. | No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Applicable legal and regulatory requirements<br>• Requirements for dealing with vulnerabilities, security incidents and malfunctions<br>• Specifications for the contractual agreement of these requirements<br>• Specifications for the monitoring of these requirements<br>• Specifications for applying these requirements also to service providers used by the third-parties, insofar as the services provided by these service providers also contribute to the provision of the cloud service | Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | Inspected the completed third-party attestation reports including review for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | No exceptions noted. |
| | | A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. | Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements. | No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SSO-02 | Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of third-parties prior to contributing to the delivery of the cloud service. The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the Cloud Service Provider during service usage.<br><br>The risk assessment includes the identification, analysis, evaluation, handling, and documentation of risks with regard to the following aspects:<br>• Protection needs regarding the confidentiality, integrity, availability, and authenticity of information processed, stored, or transmitted by the third-party<br>• Impact of a protection breach on the provision of the cloud service<br>• The Cloud Service Provider's dependence on the service provider or supplier for the scope, complexity and uniqueness of the service purchased, including the consideration of possible alternatives | Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.<br><br>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.<br><br>Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.<br><br>A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. | Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.<br><br>Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.<br><br>Inspected the vendor risk assessment policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings are approved by management.<br><br>Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SSO-03 | The Cloud Service Provider maintains a directory for controlling and monitoring the service providers and suppliers who contribute services to the delivery of the cloud service. The following information is maintained in the directory:<br>• Company name<br>• Address<br>• Locations of data processing and storage<br>• Responsible contact person at the service provider/supplier<br>• Responsible contact person at the cloud service provider<br>• Description of the service<br>• Classification based on the risk assessment<br>• Beginning of service usage<br>• Proof of compliance with contractually agreed requirements<br><br>The information in the list is checked at least annually for completeness, accuracy and validity. | The entity annually maintains and reviews a listing of all active vendors that includes basic vendor information and contractual requirements. | Inspected the completed vendor management tracking sheet and vendor listing to determine that the entity annually maintained and reviewed a listing of all active vendors that included basic vendor information and contractual requirements. | No exceptions noted. |
| | | Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | Inspected the completed third-party attestation reports including review for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | No exceptions noted. |
| | | The entity reviews its third-party relationships on an annual basis to help ensure contractual requirements and compliance obligations are being met. | Inspected the completed vendor management tracking sheet and vendor listing to determine that the entity reviewed its third-party relationships on an annual basis to help ensure contractual requirements and compliance obligations were being met. | No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SSO-04 | The Cloud Service Provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and instructions concerning controlling and monitoring of third-parties.<br><br>Monitoring includes a regular review of the following evidence to the extent that such evidence is to be provided by third-parties in accordance with the contractual agreements:<br>• Reports on the quality of the service provided<br>• Certificates of the management systems' compliance with international standards<br>• Independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems<br>• Records of the third-parties on the handling of vulnerabilities, security incidents and malfunctions<br><br>*Continues on the next page.* | The entity annually maintains and reviews a listing of all active vendors that includes basic vendor information and contractual requirements.<br><br>Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.<br><br>The entity reviews its third-party relationships on an annual basis to help ensure contractual requirements and compliance obligations are being met. | Inspected the completed vendor management tracking sheet and vendor listing to determine that the entity annually maintained and reviewed a listing of all active vendors that included basic vendor information and contractual requirements.<br><br>Inspected the completed third-party attestation reports including review for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.<br><br>Inspected the completed vendor management tracking sheet and vendor listing to determine that the entity reviewed its third-party relationships on an annual basis to help ensure contractual requirements and compliance obligations were being met. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | The frequency of the monitoring corresponds to the classification of the third-party based on the risk assessment conducted by the Cloud Service Provider (cf. SSO-02). The results of the monitoring are included in the review of the third-party's risk assessment.<br><br>Identified violations and deviations are subjected to analysis, evaluation and treatment in accordance with the risk management procedure (cf. OIS-07). | A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. | Inspected the vendor risk assessment policies and procedures and the completed vendor risk assessment for a sample of vendors to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements. | No exceptions noted. |

| CONTROL DOMAIN: CONTROL AND MONITORING OF SERVICE PROVIDERS AND SUPPLIERS (SSO) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SSO-05 | The Cloud Service Provider has defined and documented exit strategies for the purchase of services where the risk assessment of the service providers and suppliers regarding the scope, complexity and uniqueness of the purchased service resulted in a very high dependency (cf. Supplementary Information).<br><br>Exit strategies are aligned with operational continuity plans and include the following aspects:<br>• Analysis of the potential costs, impacts, resources, and timing of the transition of a purchased service to an alternative service provider or supplier<br>• Definition and allocation of roles, responsibilities, and sufficient resources to perform the activities for a transition<br>• Definition of success criteria for the transition<br>• Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable | The entity has defined termination procedures for third-party relationships in the event third-parties are not operating to management's standards and expectations.<br><br>Documented policies and procedures addressing business continuity and security incident response are in place in the event a critical third-party relationship is abruptly terminated. | Inspected the vendor management policies and procedures to determine that the entity had defined termination procedures for third-party relationships in the event third-parties were not operating to management's standards and expectations.<br><br>Inspected the business continuity plan to determine that documented policies and procedures addressing business continuity and security incident response were in place in the event a critical third-party relationship was abruptly terminated. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: SECURITY INCIDENT MANAGEMENT (SIM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SIM-01 | Policies and instructions with technical and organizational safeguards are documented, communicated, and provided in accordance with SP-01 to ensure a fast, effective, and proper response to all known security incidents. | Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | No exceptions noted. |
| | The Cloud Service Provider defines guidelines for the classification, prioritization and escalation of security incidents and creates interfaces to the incident management and business continuity management. | The incident response policies and procedures define the classification of incidents based on its severity. | Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity. | No exceptions noted. |
| | In addition, the Cloud Service Provider has set up a "Computer Emergency Response Team" (CERT), which contributes to the coordinated resolution of occurring security incidents. | An incident response team has been established by management and is communicated to designate responsibilities in the event of an incident. | Inspected the incident response policies and procedures to determine that an incident response team had been established by management and was communicated to designate responsibilities in the event of an incident. | No exceptions noted. |
| | Customers affected by security incidents are informed in a timely and appropriate manner. | Resolution of incidents are documented within the ticket and communicated to affected users. | Inspected the supporting incident tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users. | No exceptions noted. |
| SIM-02 | Subject matter experts of the Cloud Service Provider, together with external security providers where appropriate, classify, prioritize and perform root-cause analyses for events that could constitute a security incident. | An incident response team has been established by management and is communicated to designate responsibilities in the event of an incident. | Inspected the incident response policies and procedures to determine that an incident response team had been established by management and was communicated to designate responsibilities in the event of an incident. | No exceptions noted. |

| CONTROL DOMAIN: SECURITY INCIDENT MANAGEMENT (SIM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. | Inquired of the Information Security Director regarding critical incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | No exceptions noted. |
| | | | Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution. | Testing of the control activity disclosed that there were no critical incidents during the review period. |
| SIM-03 | After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if applicable, as confirmation. | Resolution of incidents are documented within the ticket and communicated to affected users. | Inspected the supporting incident tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users. | No exceptions noted. |

| CONTROL DOMAIN: SECURITY INCIDENT MANAGEMENT (SIM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| SIM-04 | The Cloud Service Provider informs employees and external business partners of their obligations. If necessary, they agree to or are contractually obliged to report all security events that become known to them and are directly related to the cloud service provided by the Cloud Service Provider to a previously designated central office of the Cloud Service Provider promptly.<br><br>In addition, the Cloud Service Provider communicates that "false reports" of events that do not subsequently turn out to be incidents do not have any negative consequences. | Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with employees. External parties can escalate via the website.<br><br>The entity's escalation policies and procedures note that false positive incident reports will not result in negative consequences for the reporter. | Inspected the incident response policies and procedures and the entity's shared drive to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and shared with employees. External parties can escalate via the website.<br><br>Inspected the incident response policies and procedures to determine that the entity's escalation policies and procedures noted that false positive incident reports would not result in negative consequences for the reporter. | No exceptions noted.<br><br>No exceptions noted. |
| SIM-05 | Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to support agencies. The information obtained from the evaluation is used to identify recurrent or significant incidents and to identify the need for further protection. | Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints. | No exceptions noted. |

| CONTROL DOMAIN: SECURITY INCIDENT MANAGEMENT (SIM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, and IPS configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |
| | | The monitoring software is configured to alert IT personnel when thresholds have been exceeded. | Inspected the monitoring tool configurations and an example alert to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded. | No exceptions noted. |

| CONTROL DOMAIN: BUSINESS CONTINUITY MANAGEMENT (BCM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| BCM-01 | The top management (or a member of the top management) of the Cloud Service Provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They must ensure that sufficient resources are made available for an effective process.<br><br>People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging employees to actively contribute to the effectiveness of continuity and emergency management. | A business continuity and contingency plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity and contingency plans to determine that a business continuity and contingency plans were documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | No exceptions noted. |
| | | The business continuity plan is tested on an annual basis. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted. |
| | | The business continuity and contingency plans are updated based on business continuity plan test results. | Inspected the business continuity and contingency plans and completed business continuity and completed test results to determine that the business continuity and contingency plans were updated based on business continuity plan test results. | No exceptions noted. |

| CONTROL DOMAIN: BUSINESS CONTINUITY MANAGEMENT (BCM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| BCM-02 | Policies and instructions to determine the impact of any malfunction to the cloud service or enterprise are documented, communicated, and made available in accordance with SP-01. The following aspects are considered as minimum:<br>• Possible scenarios based on a risk analysis<br>• Identification of critical products and services<br>• Identify dependencies, including processes (including resources required), applications, business partners and third-parties<br>• Capture threats to critical products and services<br>• Identification of effects resulting from planned and unplanned malfunctions and changes over time<br>• Determination of the maximum acceptable duration of malfunctions<br>• Identification of restoration priorities<br><br>**Continues on the next page.* | A business continuity and contingency plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity and contingency plans to determine that a business continuity and contingency plans were documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | No exceptions noted. |
| | | The business continuity plan is tested on an annual basis. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted. |
| | | The business continuity and contingency plans are updated based on business continuity plan test results. | Inspected the business continuity and contingency plans and completed business continuity and completed test results to determine that the business continuity and contingency plans were updated based on business continuity plan test results. | No exceptions noted. |
| | | The business continuity and contingency plans are updated based on business continuity plan test results. | Inspected the business continuity and contingency plans and completed business continuity and completed test results to determine that the business continuity and contingency plans were updated based on business continuity plan test results. | No exceptions noted. |

| CONTROL DOMAIN: BUSINESS CONTINUITY MANAGEMENT (BCM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO)<br>• Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO)<br>• Estimation of the resources needed for resumption | | | |
| BCM-03 | Based on the business impact analysis, a single framework for operational continuity and business plan planning will be implemented, documented and enforced to ensure that all plans are consistent. Planning is based on established standards, which are documented in a "Statement of Applicability". | A business continuity and contingency plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity and contingency plans to determine that a business continuity and contingency plans were documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | No exceptions noted. |
| | Business continuity plans and contingency plans take the following aspects into account:<br>• Defined purpose and scope with consideration of the relevant dependencies<br>• Accessibility and comprehensibility of the plans for persons who are to act accordingly<br><br>**Continues on the next page.* | The business continuity plan is tested on an annual basis.<br><br>The business continuity and contingency plans are updated based on business continuity plan test results. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis.<br><br>Inspected the business continuity and contingency plans and completed business continuity and completed test results to determine that the business continuity and contingency plans were updated based on business continuity plan test results. | No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: BUSINESS CONTINUITY MANAGEMENT (BCM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Ownership by at least one designated person responsible for review, updating and approval<br>• Defined communication channels, roles and responsibilities including notification of the customer<br>• Recovery procedures, manual interim solutions and reference information (taking into account prioritization in the recovery of cloud infrastructure components and services and alignment with customers)<br>• Methods for putting the plans into effect<br>• Continuous process improvement<br>• Interfaces to Security Incident Management | | | |
| BCM-04 | The business impact analysis, business continuity plans and contingency plans are reviewed, updated and tested on a regular basis (at least annually) or after significant organizational or environmental changes. Tests involve affected customers (tenants) and relevant third-parties. The tests are documented, and results are taken into account for future operational continuity measures. | A business continuity and contingency plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity and contingency plans to determine that a business continuity and contingency plans were documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | No exceptions noted. |
| | | The business continuity plan is tested on an annual basis. | Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted. |

| CONTROL DOMAIN: BUSINESS CONTINUITY MANAGEMENT (BCM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | The business continuity and contingency plans are updated based on business continuity plan test results. | Inspected the business continuity and contingency plans and completed business continuity and completed test results to determine that the business continuity and contingency plans were updated based on business continuity plan test results. | No exceptions noted. |

| CONTROL DOMAIN: COMPLIANCE (COM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COM-01 | The legal, regulatory, self-imposed, and contractual requirements relevant to the information security of the cloud service as well as the Cloud Service Provider's procedures for complying with these requirements are explicitly defined and documented. | The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures. | Inspected the completed internal controls matrix and the information security policies and procedures to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures. | No exceptions noted. |
| | | Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity’s strategies and objectives. | Inspected the entity's documented objectives and strategies, policies and procedures related to the relevant statutory, regulatory, to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity’s strategies and objectives. | No exceptions noted. |

| CONTROL DOMAIN: COMPLIANCE (COM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COM-02 | Policies and instructions for planning and conducting audits are documented, communicated, and made available in accordance with SP-01 and address the following aspects:<br>• Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities<br>• Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods<br>• Logging and monitoring of activities | The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards.<br><br>Evaluations. risk assessments, control self-assessments, compliance assessments are performed by individuals with sufficient knowledge of what is being evaluated.<br><br>The business continuity plan is tested on an annual basis. | Inspected the ISO Certification to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations, and standards.<br><br>Inspected the organizational chart and issue tracker to determine that evaluations risk assessments, control self-assessments, compliance assessments were performed by individuals with sufficient knowledge of what was being evaluated.<br><br>Inspected the completed business continuity test results to determine that the business continuity plan was tested on an annual basis. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: COMPLIANCE (COM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COM-03 | Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) as well as compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01) through internal audits (cf. § 9.3 of ISO/IEC 27001).<br><br>Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18). | The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures. | Inspected the completed internal controls matrix and the information security policies and procedures to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures. | No exceptions noted. |
| | | Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity’s strategies and objectives. | Inspected the entity's documented objectives and strategies, policies and procedures related to the relevant statutory, regulatory, to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity’s strategies and objectives. | No exceptions noted. |
| | | The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards. | Inspected the ISO Certification to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations, and standards. | No exceptions noted. |
| | | Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions. | No exceptions noted. |

| CONTROL DOMAIN: COMPLIANCE (COM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| COM-04 | The top management of the Cloud Service Provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS at is performed at least once a year. | Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. | Inspected the employee performance evaluation policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies. | No exceptions noted. |
| | | The operational reports reviewed by executive management define the acceptable level of operational performance and control failure. | Inspected the cybersecurity dashboard and issue tracker to determine that the operational reports reviewed by executive management defined the acceptable level of operational performance and control failure. | No exceptions noted. |
| | | The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards. | Inspected the ISO Certification to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations, and standards. | No exceptions noted. |
| | | The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. | Inspected the organizational chart, employee performance policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics. | No exceptions noted. |

| CONTROL DOMAIN: COMPLIANCE (COM) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |

| CONTROL DOMAIN: DEALING WITH INVESTIGATION REQUESTS FROM GOVERNMENT AGENCIES (INQ) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| INQ-01 | Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken. | The entity has established policies and procedures for handling customer data in the event of government investigation. The procedures assess the authenticity and applicability of respective government investigations and will communicate reliance on the legal department for correspondence to all respective parties. | Inspected the incident management policies and procedures and the entity's data privacy binding corporate rules to determine that the entity had established policies and procedures for handling customer data in the event of government investigation, and that the procedures assessed the authenticity and applicability of respective government investigations and would communicate reliance on the legal department for correspondence to all respective parties. | No exceptions noted. |
| INQ-02 | The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service. | The entity has established policies and procedures for communicating with customers in the event of a government agency's involvement in suspected illegal activities in connection with the use of the cloud services in scope. | Inspected the incident management policies and procedures and the entity's data privacy binding corporate rules to determine that the entity had established policies and procedures for communicating with customers in the event of a government agency's involvement in suspected illegal activities in connection with the use of the cloud services in scope. | No exceptions noted. |
| INQ-03 | Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the provision that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis. | The entity has defined conditions in which government agencies are permitted access to in-scope systems/data in the event of a legal investigation. | Inspected the entity's data privacy binding corporate rules to determine that the entity had defined conditions in which government agencies were permitted access to in-scope systems/data in the event of a legal investigation. | No exceptions noted. |

| CONTROL DOMAIN: DEALING WITH INVESTIGATION REQUESTS FROM GOVERNMENT AGENCIES (INQ) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| INQ-04 | The Cloud Service Provider's procedures for setting up access to or disclosure of cloud customer data as part of an investigation requests, ensure that government agencies only have access to the data they need to investigate.<br><br>If no clear limitation of the data is possible, the Cloud Service Provider anonymizes or pseudonymizes the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request. | The entity has defined conditions in which government agencies are permitted access to in-scope systems/data in the event of a legal investigation. | Inspected the entity's data privacy binding corporate rules to determine that the entity had defined conditions in which government agencies were permitted access to in-scope systems/data in the event of a legal investigation. | No exceptions noted. |
| | | In the event of a legal investigation, data accessible to government agencies is restricted to only data required to complete the investigation. | Inspected the entity's data privacy binding corporate rules to determine that in the event of a legal investigation, data accessible to government agencies was restricted to only data required to complete the investigation. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-01 | Basic Criterion<br>The Cloud Service Provider provides cloud customers with guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud customer in the secure configuration, installation, and use of the cloud service, to the extent applicable to the cloud service and the responsibility of the cloud user.<br><br>The type and scope of the information provided will be based on the needs of subject matter experts of the cloud customers who set information security requirements, implement them or verify the implementation (e.g. IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service:<br>• Instructions for secure configuration<br>• Information sources on known vulnerabilities and update mechanisms<br>• Error handling and logging mechanisms<br>• Authentication mechanisms<br><br>*Continues on the next page.* | Confidentiality requirements are communicated to customers through a master service agreement.<br><br>Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers via updated agreements and website notices.<br><br>API documentation for the organization’s application is available on a public-facing website. | Inspected the executed contract for a sample of customers to determine that confidentiality requirements were communicated to customers through a master service agreement.<br><br>Inspected the entity's website and an example updated agreement to determine that changes to commitments and requirements relating to confidentiality were communicated to third-parties, external users and customers via updated agreements and website notices.<br><br>Inspected the organization’s front-facing resource center and technical documentation to determine that API documentation for the organization’s application was available on a public-facing website. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Roles and rights concept including combinations that result in an elevated risk<br>• Services and functions for administration of the cloud service by privileged users<br><br>The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use. | | | |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-02 | The Cloud Service Provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process.<br><br>The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities:<br>• Static Application Security Testing<br>• Dynamic Application Security Testing<br>• Code reviews by the Cloud Service Provider's subject matter experts<br>• Obtaining information about confirmed vulnerabilities in software libraries provided by third-parties and used in their own cloud service<br><br>The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them. | System changes are tested prior to implementation and types of testing performed depend on the nature of the change.<br><br>System changes are authorized and approved by management prior to implementation.<br><br>Management follows a methodical process to identify assets, associated threats and vulnerabilities, and quantifies the probability, and harm that may be inflicted. Vulnerabilities are to be addressed in a timely manner and prioritized based on severity. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.<br><br>Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were authorized and approved by management prior to implementation.<br><br>Inspected the change management policies and procedures, the risk assessment policies and procedures, and the completed risk assessment to determine that management followed a methodical process to identify assets, associated threats and vulnerabilities, and quantified the probability, and harm that could be inflicted, and that vulnerabilities were to be addressed in a timely manner and prioritized based on severity. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-03 | The Cloud Service Provider operates or refers to a daily updated online register of known vulnerabilities that affect the Cloud Service Provider and assets provided by the Cloud Service Provider that the cloud customers have to install, provide or operate themselves under the customers responsibility.<br><br>The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS).<br><br>The online register is easily accessible to any cloud customer. The information contained therein forms a suitable basis for risk assessment and possible follow-up measures on the part of cloud users.<br><br>For each vulnerability, it is indicated whether software updates (e.g. patch, update) are available, when they will be rolled out and whether they will be deployed by the Cloud Service Provider, the cloud customer or both of them together. | Management follows a methodical process to identify assets, associated threats and vulnerabilities, and quantifies the probability, and harm that may be inflicted. Vulnerabilities are to be addressed in a timely manner and prioritized based on severity. | Inspected the change management policies and procedures, the risk assessment policies and procedures, and the completed risk assessment to determine that management followed a methodical process to identify assets, associated threats and vulnerabilities, and quantified the probability, and harm that could be inflicted, and that vulnerabilities were to be addressed in a timely manner and prioritized based on severity. | No exceptions noted. |
| | | Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. | Inspected the supporting ticket for a sample of vulnerabilities identified to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions. | No exceptions noted. |
| | | Identified risks are rated using a risk evaluation process and ratings are approved by management. | Inspected the risk assessment and management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |
| | | | Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment. | Inspected the vulnerability management process policies and procedures to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment. | No exceptions noted. |
| PSS-04 | The cloud service provided is equipped with error handling and logging mechanisms. These enable cloud users to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides.<br><br>The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service:<br>• Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs)<br>• Malfunctions during processing of automatic or manual actions<br><br>**Continues on the next page.* | Network audit logging configurations are in place that include user activity and system events. | Inspected the network audit logging configurations to determine that network audit logging configurations were in place that included user activity and system events. | No exceptions noted. |
| | | Databases audit logging configurations are in place to log user activity and system events. | Inspected the databases audit logging configurations to determine that databases audit logging configurations were in place to log user activity and system events. | No exceptions noted. |
| | | Application audit logging configurations are in place to log user activity and system events. | Inspected the application audit logging configurations to determine that application audit logging configurations were in place to log user activity and system events. | No exceptions noted. |
| | | The connection between the logging server and the production environment is encrypted. | Inspected the encryption configuration for data in transit between the production environment and the logging server to determine that the connection between the logging server and the production environment was encrypted. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | • Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorization, cryptography, and communication security<br>• The logged information is protected from unauthorized access and modification and can be deleted by the Cloud Customer<br>• If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities | End users with administrative privileges is able to configure logging requirements within the in-scope application(s). | Inquired of the Information Security Director regarding privilege access to determine that end users with administrative privileges were able to configure logging requirements within the in-scope application(s).<br><br>Observed the end user privileges within the application(s) to determine that end users with administrative privileges were able to configure logging requirements within the in-scope application(s). | No exceptions noted.<br><br>No exceptions noted. |
| PSS-05 | The Cloud Service Provider provides authentication mechanisms that can force strong authentication (e.g., two or more factors) for users, IT components or applications within the cloud users' area of responsibility. | Application users are authenticated via individually assigned user accounts, passwords and MFA. | Inspected the password requirement and MFA configurations to determine that application users were authenticated via individually assigned user accounts, passwords and MFA. | No exceptions noted. |
| | These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service.<br><br>For privileged users, IT components or applications, these authentication mechanisms are enforced. | The application is configured to enforce password requirements that include:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | Inspected the application password settings to determine that application was configured to enforce password requirements that included:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| | | Privileged users to the system are required to utilize multifactor authentication. | Inspected the roles and permissions for the in-scope systems to determine that privileged users to the system were required to utilize multifactor authentication. | No exceptions noted. |
| PSS-06 | To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that at least corresponds to the state-of-the-art and is protected against known attacks. Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the Cloud Service Provider or - if technically possible - by the cloud customer. | Application account lockout configurations are in place that include:<br>• Account lockout duration<br>• Account lockout threshold | Inspected the application account lockout configurations to determine that application account lockout configurations were in place that included:<br>• Account lockout duration<br>• Account lockout threshold | No exceptions noted. |
| | | The application is configured to enforce password requirements that include:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | Inspected the application password settings to determine that application was configured to enforce password requirements that included:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | No exceptions noted. |
| | | Stored passwords are encrypted. | Inspected the encryption configurations for data at rest to determine that stored passwords were encrypted. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-07 | If passwords are used as authentication information for the cloud service, their confidentiality is ensured by the following procedures:<br>• Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days.<br>• When creating passwords, compliance with the length and complexity requirements of the Cloud Service Provider (cf. IDM-09) or the cloud customer is technically enforced.<br>• The user is informed about changing or resetting the password.<br>• The server-side storage takes place using state-of-the-art cryptographically strong hash functions in combination with at least 32-bit long salt values. | The application is configured to enforce password requirements that include:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | Inspected the application password settings to determine that application was configured to enforce password requirements that included:<br>• Password history<br>• Password age (minimum and maximum)<br>• Password length<br>• Complexity | No exceptions noted. |
| | | Stored passwords are encrypted. | Inspected the encryption configurations for data at rest to determine that stored passwords were encrypted. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-08 | The Cloud Service Provider provides cloud users with a roles and rights concept for managing access rights. It describes rights profiles for the functions provided by the cloud service. | Application administrative access is restricted to authorized personnel. | Inquired of the Information Security Director regarding administrative access to the application to determine that application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | The rights profiles are suitable for enabling cloud users to manage access authorizations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks ("need-to-know principle") and to implement the principle of functional separation between operational and controlling functions ("separation of duties"). | | Inspected the application administrator listing and access roles to determine that application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Cloud administrators are able to manage internal users and assign roles to restrict access, wherever needed. | Inspected the application administrator privileges through the in-scope application to determine that cloud administrators were able to manage internal users and assign roles to restrict access, wherever needed. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-09 | Access to the functions provided by the cloud service is restricted by access controls (authorization mechanisms) that verify whether users, IT components, or applications are authorized to perform certain actions.<br><br>The Cloud Service Provider validates the functionality of the authorization mechanisms before new functions are made available to cloud users and in the event of changes to the authorization mechanisms of existing functions (cf. DEV-06). The severity of identified vulnerabilities is assessed according to defined criteria based on industry standard metrics (e.g. Common Vulnerability Scoring System) and measures for timely resolution or mitigation are initiated. Vulnerabilities that have not been fixed are listed in the online register of known vulnerabilities (cf. PSS-02). | Application administrative access is restricted to authorized personnel.<br><br>Management follows a methodical process to identify assets, associated threats and vulnerabilities, and quantifies the probability, and harm that may be inflicted. Vulnerabilities are to be addressed in a timely manner and prioritized based on severity. | Inquired of the Information Security Director regarding administrative access to the application to determine that application administrative access was restricted to authorized personnel.<br><br>Inspected the application administrator listing and access roles to determine that application administrative access was restricted to authorized personnel.<br><br>Inspected the change management policies and procedures, the risk assessment policies and procedures, and the completed risk assessment to determine that management followed a methodical process to identify assets, associated threats and vulnerabilities, and quantified the probability, and harm that could be inflicted, and that vulnerabilities were to be addressed in a timely manner and prioritized based on severity. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-10 | If the Cloud Service offers functions for software-defined networking (SDN), the confidentiality of the data of the cloud user is ensured by suitable SDN procedures.<br><br>The Cloud Service Provider validates the functionality of the SDN functions before providing new SDN features to cloud users or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner. | Documented change control policies and procedures are in place to guide personnel in the change management process. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process. | No exceptions noted. |
| | | System changes are tested prior to implementation and types of testing performed depend on the nature of the change. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change. | No exceptions noted. |
| | | System changes are authorized and approved by management prior to implementation. | Inspected the supporting change ticket for a sample of system changes and for a sample of application changes to determine that system changes were authorized and approved by management prior to implementation. | No exceptions noted. |
| | | System changes implemented for remediating incidents follow the standard change management process. | Inspected the change management policies and procedures to determine that system changes implemented for remediating incidents followed the standard change management process. | No exceptions noted. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-11 | If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects:<br>• The cloud customer can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this cloud customer can only launch the images or containers released according to these restrictions<br>• If the Cloud Service Provider provides images of virtual machines or containers to the Cloud Customer, the Cloud Service Provider appropriately inform the Cloud Customer of the changes made to the previous version<br>• In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards | Not applicable. Cloud customers are not responsible for operating or managing virtual machines directly within the in-scope applications API or management consoles. | Not applicable. | Not applicable. |

| CONTROL DOMAIN: PRODUCT SAFETY AND SECURITY (PSS) | | | | |
|---|---|---|---|---|
| **Control ID** | **Control Specification** | **Control Activity Specified by the Service Organization** | **Test Applied by the Service Auditor** | **Test Results** |
| PSS-12 | The cloud customer is able to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.<br><br>This must be ensured by the cloud architecture. | The cloud customer is able to select the location/server where their data is housed in accordance with legal and contractual agreements prior to being granted access to the in-scope environment. | Inquired of the Information Security Director, regarding data housing location configurations to determine that the cloud customer was able to select the location/server where their data was housed in accordance with legal and contractual agreements prior to being granted access to the in-scope environment. | No exceptions noted. |
| | | | Inspected the customer server data selection screen and the signed agreement for a sample of customers to determine that the cloud customer was able to select the location/server where their data was housed in accordance with legal and contractual agreements prior to being granted access to the in-scope environment. | No exceptions noted. |
| | | Customer data is replicated to specified locations per management's defined configurations. | Inspected the customer backup replication server selection screen to determine that customer data was replicated to specified locations per management's defined configurations. | No exceptions noted. |