www.pwc.dk

Unit IT Holding A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1. January 2024 to 31. December 2024 in relation to Unit IT Holding A/S' operational services and hosting activities to customers

February 2025

Contents

1 Management's statement

The accompanying description has been prepared for customers who has used Unit IT Holding A/S' operational services and hosting activities and its auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by customers itself, when assessing the risks of material misstatements in customers' financial statements.

Unit IT Holding A/S uses B4Restore A/S and Global Connect as a subservice supplier of backup services and datacenter hosting. This report uses the carve-out method and does not comprise control objectives and related controls that subservice suppliers performs for Unit IT Holding A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

Unit IT Holding A/S confirms that:

a) The accompanying description in section 3 fairly presents the Unit IT Holding A/S' operational services and hosting activities that has processed customers' transactions throughout the period from 1. January 2024 to 31. December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to Unit IT Holding A/S' operational services and hosting activities were designed and implemented, including:

   - The types of services provided
   - The procedures, within both information technology and manual systems, by which the IT general controls were managed
   - Relevant control objectives and controls designed to achieve those objectives
   - Controls that we assumed, in the design of Unit IT Holding A/S' operational services and hosting activities, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
   - How the system dealt with significant events and conditions other than transactions
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the IT general controls.

   (ii) Includes relevant details of changes to IT general controls in relation to Unit IT Holding A/S' operational services and hosting activities during the period from 1. January 2024 to 31. December 2024

   (iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to Unit IT Holding A/S' operational services and hosting activities being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the IT general controls in relation to Unit IT Holding A/S' operational services and hosting activities that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1. January 2024 to 31. December 2024. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1. January 2024 to 31. December 2024.

Middelfart, 19 February 2025
Unit IT Holding A/S

Jess Julin Ibsen
CEO

2 Independent service auditor's assurance report on the description, design and operating effectiveness of controls

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1. January 2024 to 31. December 2024 in relation to Unit IT Holding A/S's operational services and hosting activities to customers

To: Unit IT Holding A/S, customers and their auditors.

Scope

We have been engaged to provide assurance about Unit IT Holding A/S' description in section 3 of its IT general controls in relation to Unit IT Holding A/S' operational services and hosting activities which has processed customers' transactions throughout the period from 1. January 2024 to 31. December 2024 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Unit IT Holding A/S uses B4Restore A/S and Global Connect as a subservice supplier of backup services and datacenter hosting. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore A/S and Global Connect A/S performs for Unit IT Holding A/S.

Some of the control objectives stated in Unit IT Holding A/S' description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with Unit IT Holding A/S' controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

Unit IT Holding A/S's responsibilities

Unit IT Holding A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on Unit IT Holding A/S' description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its operational services and hosting activities and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by Unit IT Holding A/S in the Management's statement section.

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

Limitations of controls at a service organisation

Unit IT Holding A/S' description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of operational services and hosting activities that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to Unit IT Holding A/S' operational services and hosting activities were designed and implemented throughout the period from 1. January 2024 to 31. December 2024;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1. January 2024 to 31. December 2024; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1. January 2024 to 31. December 2024.

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used Unit IT Holding A/S' operational services and hosting activities and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Aarhus, 19 February 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

3 System description

3.1 Introduction

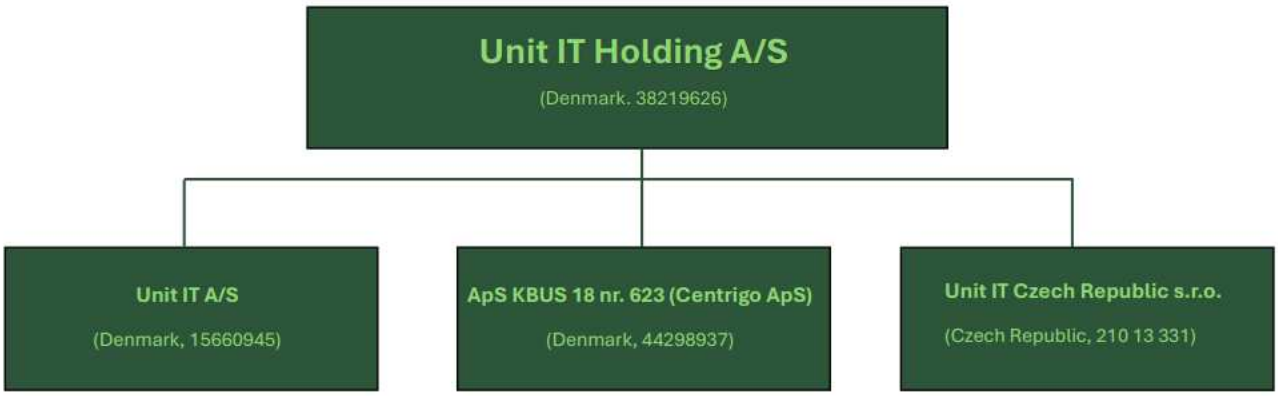
Unit IT Holding A/S (Unit IT) is a part of the USTC corporation in Middelfart. Unit IT is a managed services provider and provides a wide range of services that spans from infrastructure & cloud, managed services, consulting, data and AI services to a wide range of public and private enterprises.

Unit IT currently has two data centres in Middelfart, from here, approx. 3,000 servers are monitored and operated. Furthermore, Unit IT utilizes multiple external data centres e.g. IBM, Microsoft Azure and Global Connect.

This description is intended to report on the general controls that Unit IT implements to support and safeguard its customers.

Unit IT is organized into functional business units, operating in a structured manner aligned with the guiding and normative requirements outlined in the ISO 27000 series. This structural composition fosters an environment conducive to delivering and maintaining a consistently high level of service to Unit IT's customers. Unit IT places significant importance on achieving high service standards and ensuring customer satisfaction, recognizing these as critical elements in mitigating potential risks.

Unit IT has approximately 230 employees and is headed by Managing Director Jess Julin Ibsen, who reports to the USTC group.



- 1 March 2024: Unit IT Holding A/S acquired Global Connect Outsourcing Services (ApS KBUS 18 nr. 623), which has since been fully integrated into Unit IT Holding A/S.
- 1 April 2024: Unit IT Holding A/S established a new office in the Czech Republic (Unit IT Czech Republic s.r.o.), which also operates as an integrated part of the organization.

The entities Unit IT A/S, ApS KBUS 18, and Unit IT Czech Republic s.r.o. collectively constitute Unit IT Holding A/S.

The departments essential to Unit IT's core business and included within the scope of this audit report are as follows:

- Cloud: A consulting business specializing in cloud services, offering advisory, implementation, and optimization of cloud solutions for businesses.

- Platform: The Platform department are responsible for the technical platform, which is placed in our data center or at our customers location. The most important task is to ensure a performing, modern, financially attractive and reliable platform, to our customers benefit. The Platform team takes care of the entire lifecycle management, provide 2nd and 3rd level support, provide monitoring

to ensure the optimal foundation (Platform) for the entire Unit IT's delivery to our customers. Employees are organized into 3 teams Backup, VMware and Network/Firewall.

- Managed service: The Managed Service Department is dedicated to ensuring the robust and efficient operation of our IT infrastructure. This department is responsible for a wide range of critical tasks, including overseeing the HyperV platform and associated services to ensure optimal performance and reliability, implementing and managing software updates and patches for the HyperV platform, including continuous development of the patch management platform, managing operating systems and middleware, handling the transfer of virtual servers on the HyperV platform, ensuring minimal disruption and maximum efficiency and managing Defender Antivirus to protect systems from threats and vulnerabilities. This department plays a pivotal role in maintaining the integrity and performance of our IT services, driving innovation, and ensuring that our infrastructure meets the evolving needs of the organization.

- Service Operation: If the Service Desk cannot resolve the ticket, it is responsible for ensuring the ticket is promptly escalated to the appropriate Technical Team. This ensures that experts and specialists address the assigned task within the agreed-upon deadline.

- Support: The primary function of this team is to provide user support for the hosted solutions, including support of PCs and MAC, as well as addressing general customer questions. The Support team operates on a two-shift basis and is thus physically manned from 6 a.m. to 9 p.m. All employees offer support in Danish and English. Unit IT Holding A/S provides first level user support to more than 5,000 users.

- Operation CZ: Unit IT Czech Republic has been established to improve services and ensure that Unit IT continue to deliver the highest quality. Unit IT Czech Republic is 100% owned by Unit IT Holding A/S, and its employees are considered colleagues and partners that assist the Danish Operations department in delivering high quality service according to contractual obligations. We have ensured that Unit IT Czech Republic meets all relevant requirements under GDPR and our own stringent security standards.

- Service Delivery Management: Ensures that services agreed in the contract are delivered in due time and at the agreed quality. Service Delivery Management handles all reporting of operational services as well as KPI and SLA metrics. Furthermore, the team holds operating status and steering group meetings with customer and supplier representatives. Service Delivery Management is also the escalation point in case of disputes and acts as Situation Manager 24/7 in case of critical incidents. If requested by the customer, Service Delivery Management acts as a trusted advisor to the customer and as a coordinator between the customer and third-party suppliers.

- Security: The primary functions provided by the security teams, is to ensure that appropriate governance, risk management and compliance are in place and to guard information, system and networks from cyber-attacks (Cyber Defence Center). Security performs everything from maturity and risk assessments to 24/7 monitoring and technical security.

Except for the organizational changes described above, there has been no major changes to procedures and internal controls during the period from 1. January to 31. December 2024.

3.2 Control environment

The determination for establishing the control environment is based on ISO27001:2022 – Annex A, referenced in ISO27002. Unit IT A/S and Global Connect Outsourcing Services are ISO27001 certified, ensuring a structured approach to risk management across the four control domains: organizational, personnel-related, physical, and technological controls. Both certificates are available from our website.

Our approach to implementing controls is based on the guidelines outlined in ISO 27002:2022. Unit IT has focused on the following four security control domains:

- Organizational controls

- People controls
- Physical controls
- Technological controls

Organizational controls

Unit IT has defined an 'Information security policy' that all employees must follow. The policy is reviewed at planned intervals, defines the framework for the ISMS and outlines responsibilities for information security. This framework is designed to manage and oversee the implementation and operation of the information security management system (ISMS), which is certified by an accredited body.

Unit IT also maintains an asset inventory (CMDB) identifying assets and the corresponding criticality and interdependencies. Unit IT monitors critical assets using a SIEM solution to ensure early identification of security incidents. All critical assets are risk assessed.

Unit IT has established a process to oversee its subservice suppliers, incorporating a set of controls to ensure regular monitoring of the suppliers' compliance with agreed contractual obligations. These controls include, but are not limited to:

- If applicable in accordance with the criticality of the sub-supplier and sub-processor, an annual collection of ISAE or SOC reports from the subservice supplier's independent body.
- If applicable in accordance with the criticality of the sub-supplier and sub-processor, an annual collection of their ISO27001 certificate.

Unit has established a process for incident management and information security handling, supported by a comprehensive set of controls to ensure a timely, effective, and consistent response to incidents, security events, and vulnerabilities. In alignment with ISO 22301, Unit IT incorporates business continuity planning, which involves planning and testing for potential disruptions at regular intervals (at least annually). Additionally, controls for responsibility and communication are in place and are tested periodically.

Unit IT has implemented a set of controls to ensure that legal and contractual obligations are regularly reviewed and selected controls have been implemented to meet the required standards. These controls include, but are not limited to:

- Organizational responsibility to assess and monitor Unit IT's capabilities.
- Applicable laws and regulation have been identified.
- Privacy and PII has been identified and several selected controls have been implemented to limit (retain and delete) and protect data and analogue information.
- Information security controls are reviewed by internal audit and further backed up by independently reviews annually by an independent body.

People controls

All employees undergo mandatory training in information and cybersecurity. Training results are monitored and evaluated by management.

The Acceptable Use Policy establishes clear guidelines for the appropriate use of company IT resources, including mobile devices, computers, and external media. Employees are required to adhere to these guidelines. This policy also governs the use of the company's network and applications, emphasizing secure and responsible behaviour.

Access rights to information systems are granted strictly on a need-to-know basis, following the principle of least privilege. Role-based access controls ensure that employees only have access to the resources necessary for their duties. Access rights are periodically reviewed to maintain alignment with organizational responsibilities.

Physical controls

Unit IT has implemented comprehensive physical and organizational controls to ensure the security and resilience of its hosting and housing facilities. Access to these facilities is strictly restricted to authorized personnel, with entry granted only to key staff on a need-to-know and role-specific basis. Access controls are strengthened through a combination of physical barriers, including secure locks, biometric authentication, and CCTV surveillance, alongside logical access systems to provide thorough protection against unauthorized access.

To reduce environmental risks, the facilities are equipped with advanced protections against fire, lightning, flooding, and other natural disasters. Fire suppression systems, water detection sensors, and climate control mechanisms are installed and regularly maintained to ensure their effectiveness

The facilities are designed with redundancy to guarantee high availability and service continuity. This includes backup power systems, such as uninterruptible power supplies (UPS) and generators, as well as redundant cooling systems to maintain optimal conditions during equipment or utility failures. Surge protection mechanisms are in place to protect equipment from power grid fluctuations or spikes.

Continuous monitoring is conducted 24/7 using integrated surveillance systems, security personnel, and automated alerts, ensuring rapid detection and response to potential threats or anomalies.

To assess the effectiveness of these controls, Unit IT undergoes regular audits and assessments by independent accredited bodies, at least annually. This ensures alignment with industry best practices and compliance with ISO 27002:2022.

Technological controls

Unit has established robust controls to ensure a structured and consistent approach to user rights administration and access management. Access to systems is governed by the principle of least privilege, granting users only the minimum necessary access to perform their roles. Any elevation of access rights requires formal management approval. The creation of privileged accounts follows a strict process that includes the four-eyes principle (Segregation of Duties - SoD).

Access credentials, including usernames and passwords, comply with stringent policies that enforce complexity requirements and periodic password rotations to minimize the risk of compromise. User accounts and access permissions are regularly reviewed to ensure they remain appropriate, with unnecessary access revoked promptly.

To maintain the integrity of system security, technical access controls are implemented across all systems to prevent unauthorized or forceful login attempts. System access activities are continuously monitored by a Security Information and Event Management (SIEM) solution, which routes alerts on abnormal events to the Cyber Defence Center (CDC) for immediate investigation and response

Unit IT has also implemented comprehensive cryptographic controls to protect data both in transit and at rest. These controls are tailored to the infrastructure and security requirements of the specific environment, ensuring compliance with regulatory and contractual obligations.

Secure Operations and Change Management
Unit IT has established and documented operational procedures to ensure secure and consistent system operations. These procedures cover the management of contractual obligations, mitigation of operational risks, and compliance with security standards. Specific measures include:

- Change Management: All changes to systems are subject to a stringent approval process via the Change Advisory Board (CAB), which includes input from the customer or X, as applicable. This ensures that changes are thoroughly reviewed and aligned with security policies.
- Malware Protection: Systems are safeguarded against malware and viruses through the deployment of updated protective measures and real-time scanning.

- Backup and Recovery: Regular backups are performed, tested periodically for reliability, and stored securely in offsite locations for redundancy.

Systems and devices are continuously monitored for vulnerabilities, with any findings incorporated into the SIEM for centralized tracking and remediation planning.

Network and System Security
Unit IT implements a range of measures to safeguard information networks and processing facilities. Networks and associated equipment are closely controlled, managed, and continuously monitored. Firewalls are configured to permit only the minimum necessary traffic, adhering to the principle of least privilege for IP and port access. Networking devices are regularly updated with patches to address vulnerabilities identified by manufacturers.

Unit IT systems undergo periodic vulnerability scans to proactively identify and mitigate potential weaknesses.

The focus on strong access management, secure operations, and proactive monitoring enhances the overall resilience of Unit IT's information systems and networks.

3.3 Risk management

Top management holds ultimate responsibility for Unit IT's information security and risk management. The core principle is that information security is grounded in the actual risks the company is exposed to.

Unit IT's utilizes 2 different risk methodologies. Initially ISO27001 risk assessments are based on the implementation guidelines in ISO31010 and ISO27005 subsequently following an Octave approach.

Secondly, a customized approach for assessing risks related to software vulnerabilities has been implemented across the organization. This method addresses specific risks that cannot be effectively managed using the previously mentioned methodologies, such as Octave and ISO 27001, in day-to-day operations. It leverages tailored impact assessments and mitigations to ensure comprehensive risk management.

Unit IT has a formal, management-approved process for risk management that results in action plans. These action plans are assigned and addressed in accordance with the risk treatment process.

The initial Octave risk analysis involves a hypothetical assessment of the consequence (extent) which may negatively affect Unit IT and the probability that a given incident manifests itself through the exploitation of vulnerabilities. The analysis is used to identify the potential risks where Unit IT should implement mitigating measures, and a plan is drawn up that can reduce the risk to an acceptable level.

Progress and deviations are regularly communicated to the Security Committee so that deviations and exceptions can be identified and addressed as part of management's review of risk management activities. Security validates results and the CISO reports to the Security Committee about metric changes in Security score, CMMI score as well as risk and BIA scale changes in relation to Risk.

All critical systems/information assets from ISO31010 BIA must be reviewed annually. Non-critical systems/information assets are assessed during implementation, as well as in the event of major changes in the organization, e.g. acquisitions, relocation of offices, changes in the technical infrastructure, or introduction of new or changed IT services which are estimated to affect Unit IT's business or ability to be in control of critical assets.

A more detailed description of implemented measures appears in section 4 on the description of our control objectives and related controls as well as the auditor's description of the test of controls for this assurance report.

3.4 Complementary controls at customers

As part of the service delivery, the customer must implement and properly manage specific controls necessary to achieve the control objectives outlined in the description. These controls include, but are not limited to:

- Consider and test new versions of systems during the implementation stage.
- Ensure that systems in operation can be patched and updated following the manufacturer's instructions
- Inform Unit IT about access management requirements in connection with setting up and managing its own users in the production environment.
- If relevant, manage the setup and administration of users from Unit IT and external suppliers who assist in the customer's environments.
- Ensure that all necessary data is included in support cases.
- Inform Unit IT of any changes in employees with access to shared sites between the customer and Unit IT.
- Ensure that the contingency plan cover all critical systems and communicate to Unit IT which systems need to be disaster recovery-tested and the frequency of such tests.
- Unit has implemented controls to ensure data is backed up, and backup copies are available for restoration.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", and additional requirements applicable in Denmark.

Our testing of the design, implementation and functionality of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2 Test actions

The test actions performed when determining the operating effectiveness of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned during the period from 1. January 2024 to 31. December 2024. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed.

4.3 Overview of control objectives, control activity, tests and test results

Control objective 5:
Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.1	**Policies for information security** *Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.* Unit IT has defined and documented a policy for information security. The policy is approved by management and reviewed once a year and if significant changes occur. The policy is communicated to all employees and to other relevant parties. Unit IT has also defined other topic-specific policies to support Unit IT's approach to manage information security.	We have inquired regarding the procedures/control activities performed. We have inspected that a Management-approved and updated security policy is in place. We have inspected that the information security policies are communicated to employees and relevant parties.	No exceptions noted.
5.2	**Information security roles and responsibilities** *Information security roles and responsibilities should be defined and allocated according to the organization needs.* Unit IT has defined and documented a policy for Information Security Governance. This policy is to set out the governance of information security within Unit IT, including the composition, scope, roles and responsibilities of the information security organisation. The reporting structure, which shall ensure adherence to the policy, is also included.	By inspection, we have observed that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No exceptions noted.

Control objective 5:

Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.3	**Segregation of duties** *Conflicting duties and conflicting areas of responsibility should be segregated.* Unit IT Group's Information Security Management System (ISMS) defines the governance, roles and responsibilities and intent of the information security work at Unit IT. Unit IT has implemented their information security work according to the principle of three line of defence to ensure that duties are segregated. The first line of defence is provided by line management, the risk owners and the employees. The second line of defence is provided by the information security organisation and the third line of defence is provided by Internal Audit.	By inspection of random samples, we have investigated that the critical operating functions at Unit IT have been appropriately segregated and that primary and secondary operating data have been segregated.	No exceptions noted.
5.4	**Management responsibilities** *Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.* Unit IT's management has the overall responsibility for information security and that all personnel are aware of and fulfil their information security responsibilities.	We have inquired regarding the procedures/control activities performed. We have inspected that the information security policies are communicated to employees and relevant parties.	No exceptions noted.

Control objective 5:

Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.7	**Threat intelligence** *Information relating to information security threats should be collected and analysed to produce threat intelligence.* Unit IT identifies intelligence needs through stakeholder interviews, creating general intelligence requirements, priority intelligence requirements and focused collection requirements. Intelligence is collected from internal and external sources and disseminated to various end-users and in various formats like technical integrations, reports, and briefings.	By inspection, we have observed that information relating to information security threats is collected and analysed.	No exceptions noted.
5.9	**Inventory of information and other associated assets** *An inventory of information and other associated assets, including owners, should be developed and maintained.* Unit IT has implemented and maintains multiple CMDBs depending on the nature of the assets in scope. This includes, but not limited to, servers, network equipment, databases, PCs, laptops as well as mobile devices. Assets are assigned owners, criticality and other relevant information. Furthermore, all internal assets are reviewed once year and risk assessed if deemed critical.	We have inquired regarding the procedures/control activities performed. We have inspected that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.	No exceptions noted.

Control objective 5:
Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.15	**Access control** *Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.* Unit IT has implemented an access control policy and supplementary guidelines for access controls. Unit IT follows a least privilege access privilege and users are only granted access based on a work-related need. Processes for access provisioning, access review and access revoking has been implemented for users managed by Unit IT.	We have inquired regarding the procedures/control activities performed. We have inspected that guidelines on access controls have been implemented, reviewed and approved.	No exceptions noted.
5.16	**Identity management** *The full life cycle of identities should be managed.* Unit IT has established processes to ensure that identification of individuals are managed appropriately. Access to Unit IT information systems is only allowed after provision of a unique user ID and password.	We have inquired regarding the procedures/control activities performed. We have inspected that procedures include the full life cycle of an identity.	No exceptions noted.

Control objective 5:

Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.17	**Authentication information** *Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.* Unit IT has implemented a formalized process to manage authentication information by leveraging alternative, secure methods e.g. to verify user identity without requiring traditional passwords. These methods typically involve possession-based factors (e.g., cryptographic tokens, biometrics, or email-based links).	By inspection, we have observed that has established formalised procedures for user administration and rights management. We have observed that authorisations granted at Unit IT include an access request justification.	No exceptions noted.
5.18	**Access rights** *Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.* Unit IT has established access controls to ensure that user provisioning, user review and removal of user access is performed according to Unit IT's policies. Unit IT follows a least privilege access privilege and users are only granted access based on a work-related need.	By inspection, we have observed that user access rights are reassessed once every six months.	No exceptions noted.

Control objective 5:
Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.19	**Information security in supplier relationships** *Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.* Unit IT has established and implemented processes and procedures to identify and manage information security risks associated with the use of suppliers. Unit IT performs a yearly criticality assessment of critical suppliers supplemented with a due diligence to ensure that suppliers meet the requirements of Unit IT.	We have observed that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements.	No exceptions noted.
5.22	**Monitoring, review and change management of supplier services** *The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.* Unit IT has established procedures for managing security risks associated with the use of a supplier's products and services, which include a risk assessment of new critical suppliers followed by an assessment and audit of suppliers to ensure that the supplier continues to meet the security requirements that Unit IT expects. If changes to supplier services affect customer environments, services or infrastructure, these are managed according to Unit IT's internal processes.	We have observed that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From a sample of signed contracts, we observed that information security requirements have been contractually agreed. We have observed that Unit IT audits key suppliers on a periodic basis, based on agreed information security requirements. We have observed that third-party declarations have been received and processed by Unit IT for key suppliers.	No exceptions noted.

Control objective 5:
Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.24	**Information security incident management responsibilities and preparation** *The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.* Unit IT has defined, established and implemented procedures and processes for information security incidents. Roles and responsibilities related to incident responses has been clearly defined and communicated to all relevant employees.	We have observed that a formal and documented incident management process related to information security events and breaches has been implemented. We have observed that the incident management processes has been communicated to employees. We have observed that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system and reported through the Information Security Board.	No exceptions noted.
5.29	**Information security during disruption** *The organization should plan how to maintain information security at an appropriate level during disruption.* Unit IT has established business continuity plans to maintain an appropriate level of information security and operating activities in case of a disruption. Furthermore Unit IT has a topic specific Incident Response Plan outlining specific tasks and roles during an information security incident.	We have inquired regarding the procedures/control activities performed. We have inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually. We have inspected that a business impact assessment has been performed to establish the requirements of a business continuity plan. We have inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No exceptions noted.

Control objective 5:

Organizational Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.37	**Documented operating procedures** *Operating procedures for information processing facilities should be documented and made available to personnel who need them.* Unit IT has established and documented operating procedures to support the operating activities in Unit IT and operating activities delivered by Unit IT to customers. The operating procedures are communicated and made available for all employees in Unit IT with a work-related need.	We have inquired regarding the procedures/control activities performed. We have inspected that operating procedures have been established and that these are subject to updating at least once a year. We have inspected that the operating procedures are accessible to all relevant employees.	No exceptions noted.

Control objective 6:

People Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
6.1	**Screening** *Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.* Unit IT has defined and documented a policy for personnel security. Personnel security management controls are performed before, during and after employment where considered relevant and according to applicable laws, regulations and business requirements.	We have inquired regarding the procedures/control activities performed. We have inspected that an HR process is in place to ensure that criminal records are presented before employment starts for both employees and external consultants. Using samples, we have inspected that criminal records have been acquired before employment starts for new hires.	We have observed during our audit that there is a lack of verification and screening of employees in connection with employment. However, Unit IT has drawn up a procedure for the same, which is why we expect that the observation will be removed for the next period. No further exceptions noted.
6.2	**Terms and conditions of employment** *The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.* Responsibilities for information security is clearly defined in all employment contracts between the company and the employee.	Using random samples, we observed that confidentiality agreements are used in accordance with the guidelines, including: • that employees sign confidentiality agreements at the time of employment • that external consultants sign confidentiality agreements prior to starting work.	We have observed that one user in the inspected sample do not have a signed contract/NDA. No further exceptions noted.

Control objective 6:

People Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
6.3	**Information security awareness, education and training** *Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.* Unit IT has established information security awareness, education and training programmes for all employees. The information security awareness, education and training programme is performed throughout the year. Training results are monitored and evaluated by management.	We have observed that Unit IT runs introductory courses for new employees during which information security requirements are explained. We have observed that employees are enrolled in mandatory training programmes at regular intervals for the purpose of ensuring compliance with the security requirements of the organisation.	No exceptions noted.

Control objective 7:

Physical Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
7.1	**Physical security perimeter** *Security perimeters should be defined and used to protect areas that contain information and other associated assets.* Unit IT has defined physical security perimeters for all buildings containing information processing facilities.	We have inquired regarding the procedures/control activities performed. We have inspected that a formal physical access and security policy is maintained, reviewed and approved. We have inspected the physical security controls at the facilities.	No exceptions noted.
7.2	**Physical entry** *Secure areas should be protected by appropriate entry controls and access points.* Unit IT has established physical access controls to secure areas. These controls include: identification cards, registration of visits and constant supervision of approved and cleared employees.	We have inquired regarding the procedures/control activities performed. We inspected that a formal physical access and security policy is maintained, reviewed and approved. We have inspected the physical security controls at the facilities We have observed that Unit IT has implemented appropriate entry controls to protect physical facilities.	No exceptions noted.
7.3	**Securing offices, rooms and facilities** *Physical security for offices, rooms and facilities should be designed and implemented.* Unit IT has established appropriate measures to offices, data centres and other facilities that processes sensitive information.	By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. We have inspected the physical security controls at the facilities We have observed that Unit IT has implemented appropriated entry controls to protect physical facilities.	No exceptions noted.

Control objective 7:
Physical Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
7.4	**Physical security monitoring** *Premises should be continuously monitored for unauthorized physical access.* Unit IT has established access controls to datacentres to prevent and detect unauthorized physical access to the premises. Unit IT has installed video monitoring systems in all critical datacentres. Datacentres are monitored 24/7 365.	We have inquired regarding the procedures/control activities performed. We have inspected that Unit IT has obtained an audit report from a subcontractor and that they have viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	No exceptions noted.
7.5	**Protecting against physical and environmental threats** *Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.* Unit IT has established appropriate measures to offices, data centres and other facilities that processes sensitive information to protect against physical and environmental threats. Appropriate internal controls have been implemented to mitigate risks of potential physical and environmental threats.	We have inquired regarding the procedures/control activities performed. We have inspected that Unit IT has obtained an audit report from a subcontractor and that they have viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	No exceptions noted.
7.8	**Equipment siting and protection** *Equipment should be sited securely and protected.* Unit IT has established access controls to datacentres to prevent and detect unauthorized physical access or suspicious behaviour.	We have observed that a formal and documented incident management process related to information security events and breaches has been implemented. We have observed that the incident management processes have been communicated to employees.	No exceptions noted.

Control objective 7:

Physical Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
7.12	**Cabling security** *Cables carrying power, data or supporting information services should be protected from interception, interference or damage.* Cables supplying power as well as transmission cables (RJ45 & fibers) are containerized, in the quest for resiliency.	By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. We have observed that Unit IT has implemented appropriate controls to protect physical facilities and cabling security.	No exceptions noted.
7.14	**Secure disposal or re-use of equipment** *Equipment should be sited securely and protected.* Unit IT has implemented guidelines for disposal or recycling of equipment. This ensures that storage medias are disposed of through a certified supplier.	We have inquired regarding the procedures/control activities performed. We have inspected that Unit IT has implemented procedures on secure disposal or re-use of equipment. We have inspected that Unit IT has implemented relevant controls in relation to handling the operation of the operating environment.	No exceptions noted.

Control objective 8:

Technological Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.1	**User endpoint devices** *Information stored on, processed by or accessible via user endpoint devices should be protected.* Unit IT has established several controls to protect information accessed, stored and processed through user endpoint devices. These controls includes verification of device ID, use of strong authentication mechanism, encryption on hardware level, use of biometrics, secure DNS, use of privilege escalation, 24/7 365 monitoring of suspicious activity and backup of data.	We have observed that all types of identified assets, including endpoint devices, are listed in the acceptable use policy. We have observed that updates to the acceptable use policy is communicated to employees. We have observed that a process is in place to maintain an approved whitelist of allowed services and applications.	No exceptions noted.
8.2	**Privileged access rights** *The allocation and use of privileged access rights should be restricted and managed.* Privileged access is defined in Unit IUT's access control policy. An admin access is mandated through Unit IT's tiering model, only allowing admin user accounts with an escalation possibility if deemed necessary and approved by an authorised user for a time limited period.	We have inquired regarding the procedures/control activities performed. We have inspected that Unit IT has established formalised procedures for user administration and rights management and that these also apply to users with privileged rights. We have inspected that authorisation granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior.	No exceptions noted.
8.3	**Information access restriction** *Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.* Unit IT has established and implemented access controls to restrict access to systems and applications to employees who have a work-related need.	We have inquired regarding the procedures/control activities performed. We have inspected that procedures for user administration have been established. We have performed inquiries and inspected systems for logging and monitoring access controls.	No exceptions noted.

Control objective 8:

Technological Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.5	**Secure authentication** *Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.* Unit IT has established secure authentication technologies for sensitive information, which includes multi-factor authentication.	We have inquired regarding the procedures/control activities performed. We have inspected that a formal policy for access control that defines allowed technical solutions for authentication is maintained. Using samples, we have inspected that the user registration and de-registration process has been implemented.	No exceptions noted.
8.7	**Protection against malware** *Protection against malware should be implemented and supported by appropriate user awareness.* All Unit IT endpoint devices has enhanced malware protection, detection and remediation enabled. Disabling any type of protection automatically alarms Unit IT's CDC and the device subsequently is denied access to processing facilities. According to the individual customer contract Unit IT deploys anti malware on hosted servers.	We have inquired regarding the procedures/control activities performed. Using samples, we have inspected that the employees' computers managed by Unit IT are protected by anti-virus software – and that this software is up to date.	No exceptions noted.
8.8	**Management of technical vulnerabilities** *Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.* Unit IT has established a specific risk assessment policy and procedure, in order to assess vulnerabilities. Risks are assessed on an ongoing basis and mitigated in accordance to their criticality.	We have inquired regarding the procedures/control activities performed. We have inspected that risk assessment has been performed for vulnerability handling. We have inspected technical measures to secure against vulnerabilities.	No exceptions noted.

Control objective 8:

Technological Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.13	**Information backup** *Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.* All backup data are kept isolated from the processing datacentre. • For Unit IT: Minimum once a year, a test of the backup and recovery procedure for all business-critical systems is performed. • For customers: Restore tests are agreed individually based on e.g. criticality, frequency and retention period of systems and data.	We have inquired regarding the procedures/control activities performed. We have inspected that a full restore test of IT environments has been planned.	No exceptions noted.
8.14	**Redundancy of information processing facilities** *Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.* Unit IT has built in redundancy and/or automatically failover in all critical information processing facilities, and for all customers' information processing facilities according to customer specific requirements. Unit IT is alerted in case of failures in the redundant information processing facilities including datacentre.	We have observed that key operating areas have been outsourced to a supplier. We have observed that Unit IT follows up on delivered services from suppliers. We have inspected data processing facilities and systems. We have observed that the systems are implemented redundant an failover capabilities for servers, network and storage.	No exceptions noted.

Control objective 8:

Technological Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.15	**Logging** *Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.* Unit IT has implemented a policy for logging and monitoring to detect, analyse and respond to security threats through a SIEM system on all relevant internal systems and on customers' systems according to customer contracts and requirements. Segregation of duties have been implemented to protect log information. Users with access to log information do not have access to source systems.	We have inquired regarding the procedures/control activities performed. We have inspected that event logging of user activities, exceptions, faults and information security events has been configured.	No exceptions noted.
8.16	**Monitoring activities** *Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.* Unit IT has its own Cyber Defense Center (CDC) that continuously monitors processing facilities and receives and responds to potential threats.	We have inquired regarding the procedures/control activities performed. Using samples, we have inspected that logging parameters are set up to ensure that actions performed by users with extended access rights are logged.	No exceptions noted.
8.17	**Clock synchronization** *The clocks of information processing systems used by the organization should be synchronized to approved time sources.* Unit IT has synchronized all relevant information processing systems to a single reference time source.	We have inspected system configuration for network time synchronisation. We have observed that NTP have been configured. We have on sample basis inspected changes to configuration.	No exceptions noted.

Control objective 8:

Technological Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.20	**Network security** *Networks and network devices should be secured, managed and controlled to protect information in systems and applications.* The internal network is secured with physical firewalls. Communications between Unit IT office locations and the datacentres are secured via encrypted network tunnels. All changes to the configuration of the network or security measures must be tested, approved, and documented accordingly to the generally applicable change management process.	We have inspected system configurations for firewall, network switches and network topology. We have observed that the network is protected with firewalls and segregated. .	No exceptions noted.
8.22	**Segregation in networks** *Groups of information services, users and information systems should be segregated in the organization's networks.* Unit IT separates customer networks into one or more networks depending on the requirements for separation. Customers do not have access to other customer networks.	We have inspected system configurations for firewall, network switches and network topology. We have observed that the network is protected with firewalls and customer networks are segmented and isolated.	No exceptions noted.
8.24	**Use of cryptography** *Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.* Unit IT has defined and implemented rules for use of cryptography for protection of information.	We have inquired regarding the procedures/control activities performed. We have inspected that an appropriate use of secure cryptography and key management has been established.	No exceptions noted.

Control objective 8:

Technological Controls

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.32	**Change management** *Changes to information processing facilities and information systems should be subject to change management procedures.* Unit IT has established and implemented a change management process that ensures that all changes to information systems in production environments are subject to change management, which ensures that changes do not unnecessarily affect each other and that fall-back plans are in place.	We have inspected the adequacy of change management procedures and inspected that an appropriate change management system is established supported by a technical infrastructure. We have inspected that a formal change management procedure has been implemented in the organisation. Using samples we have inspected that the change management procedure is followed.	No exceptions noted.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jess Julin Ibsen
Kunde
Serienummer: c51d4162-810e-4a38-8c1b-2deada7381a0
IP: 62.243.xxx.xxx
2025-02-19 11:29:27 UTC

Mit ID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-19 11:36:19 UTC

Mit ID