Unit IT Holding A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2025 to 31 December 2025 in relation to Unit IT Holding A/S's operational services and hosting activities to customers

February 2026

Contents

1. Management's assertion

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

B4Restore A/S and Global Connect are service organisations that provide backup services and data centre hosting to Unit IT. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Unit IT and excludes the control objectives and related controls of B4Restore A/S and Global Connect. Our evaluation did not extend to controls of B4Restore A/S and Global Connect.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of our controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Unit IT confirms that:

a) The accompanying description in section 3 fairly presents the operational services and hosting activities that have processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to the 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 the 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 IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to the operational services and hosting activities during the period from 1 January 2025 to 31 December 2025

   (iii) Does not omit or distort information relevant to the scope of IT general controls in relation to the 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 IT general controls in relation to the 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 2025 to 31 December 2025. 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

(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 2025 to 31 December 2025.

Middelfart, 5 February 2026
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 2025 to 31 December 2025 in relation to Unit IT's operational services and hosting activities to customers

To: Unit IT Holding A/S (Unit IT), its customers and their auditors

Scope

We have been engaged to report on Unit IT's description in section 3 of IT general controls in relation to the operational services and hosting activities which have processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Unit IT uses B4Restore A/S and Global Connect for its backup services and data centre hosting. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Unit IT and excludes the control objectives and related controls of B4Restore A/S and Global Connect. Our examination did not extend to controls of B4Restore A/S and Global Connect.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of Unit IT's controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Unit IT's responsibilities

Unit IT is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria 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 the fairness of Unit IT's description and on the suitability of 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 comply with ethical requirements and 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 of a service organisation's system and the suitability of the design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the description 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 also 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 by Unit IT and described in section 1.

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

Inherent limitations

Unit IT'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 the operational services and hosting activities that the individual customer may consider important in its own particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in the operational services and hosting activities. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria including the control objectives described in Unit IT's assertion in section 1:

a) The description fairly presents how IT general controls in relation to the operational services and hosting activities were designed and implemented throughout the period from 1 January 2025 to 31 December 2025

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2025 to 31 December 2025 and user entities applied the complementary customer controls referred to in section 3

c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, 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 2025 to 31 December 2025.

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

We were engaged to report by Unit IT and, therefore, this report and the description of tests of controls and results thereof in section 4 are intended for the use of Unit IT.

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Unit IT, at its discretion, to customers who have used Unit IT's operational services and hosting activities during some or all of the period of 1 January 2025 to 31 December 2025 and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

Our report is not to be used for any other purpose or to be distributed to any other parties.

Aarhus, 5 February 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen State-Authorised Public Accountant mne26801	Rico Lundager Director

3. System description

3.1. General description of Unit IT Holding A/S

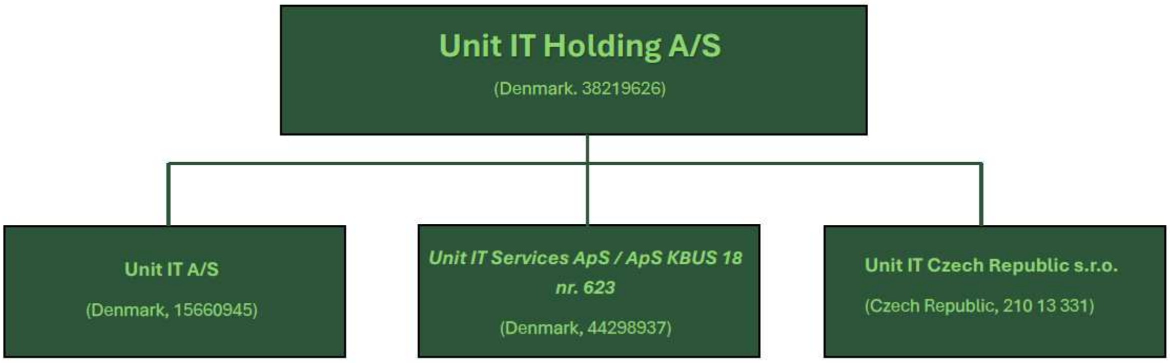
Unit IT Holding A/S (Unit IT) is a part of the USTC corporation in Middelfart. Unit IT is a managed services provider and provides a wide range of services that range from Infrastructure, Cloud, Managed Services, Consulting, Data and AI services to a wide range of public and private enterprises.

Unit IT currently has two data centres in Middelfart. From here, approx. 3,000 servers are monitored and operated. Furthermore, Unit IT utilises 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 organised 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, recognising 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.


Unit IT Holding A/S
(Denmark. 38219626)
Unit IT A/S
(Denmark, 15660945)
Unit IT Services ApS / ApS KBUS 18 nr. 623
(Denmark, 44298937)
Unit IT Czech Republic s.r.o.
(Czech Republic, 210 13 331)

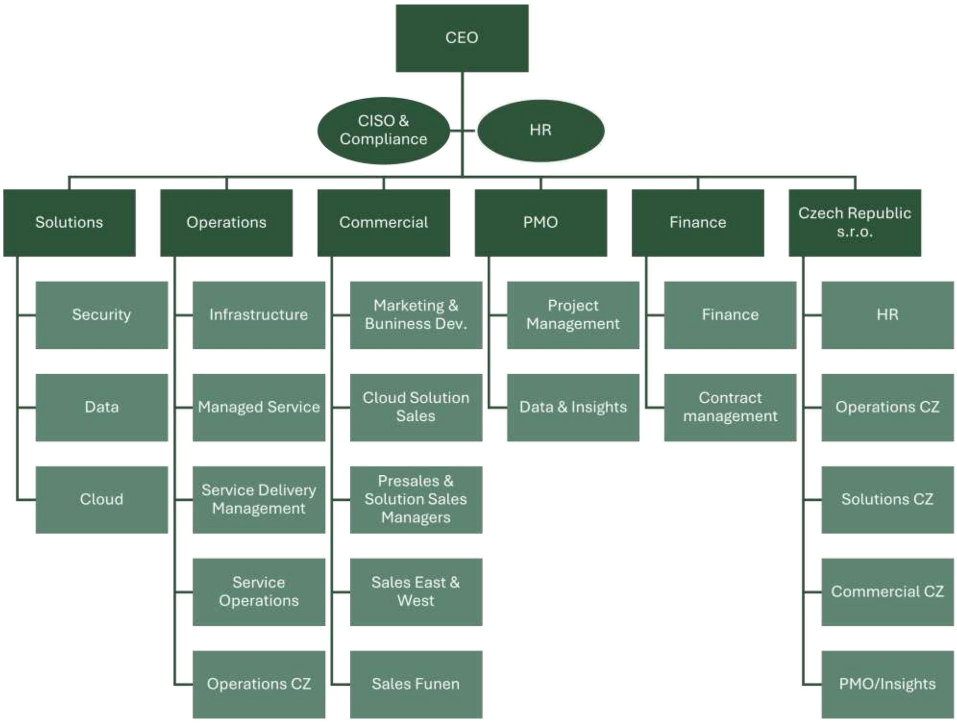
- 1 March 2024: Unit IT Holding A/S acquired Global Connect Outsourcing Services (ApS KBUS 18 nr. 623), which has since been fully integrated into Unit IT Holding A/S.
- 1 April 2024: Unit IT Holding A/S established a new office in the Czech Republic (Unit IT Czech Republic s.r.o.), which also operates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

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

This assurance report covers Unit IT Holding A/S and, consequently, its three legal entities; Unit IT A/S, Unit IT Services ApS and Unit IT Czech Republic s.r.o.

This independent assurance report focuses on Unit IT's core business within the Operations business unit. Additionally, the scope of this assurance report also includes Unit IT's Cloud and Security, with focus on the Cyber Defense Center, within the Solutions business unit. The equivalent business units under Czech Republic s.r.o. are also in scope for this assurance report.

Furthermore, both HR and CISO and Compliance are included in the scope of the assurance report as supporting business units.



Unit IT organisation chart

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 specialising in cloud services, offering advisory, implementation and optimisation of cloud solutions for businesses.

- Infrastructure: The Infrastructure department is responsible for the technical platform, which is placed in our data centre 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 organised into three teams: Backup, VMware and Network/Firewall.

- Managed services: 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 organisation.

- Service Operations: The primary function of this team is to provide user support for the hosted solutions, including support of PCs and MACs, 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 provides first level user support to more than 5,000 users.

- Operations CZ: Unit IT Czech Republic has been established to improve services and ensure that Unit IT continues 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 service in Unit IT's Security department is the Cyber Defence Center. The Cyber Defence Center provides an integrated security solution, bringing traditional security services together in one place. The focus is on quality, value and strengthening the organisation's defence against advanced threats. The Cyber Defence Center offers AI-driven security operations services through a newly implemented SIEM, that supports centralisation of data and automation of threat detection. The solution supports critical incident repsonse and generates alerts in the event of security breaches, with monitoring available around the clock (24/7). In addition, the CDC supports with security awareness training, DMARC configuration, Zero Trust implementation, and advisory services in the event of security incidents – all designed to build a robust, proactive and value-adding cybersecurity defence.

- CISO and Compliance: The CISO and Compliance department provides an integrated approach to governance, risk and compliance, ensuring that information security management is embedded throughout the organisation. The focus is on maintaining and continuously improving the information security management system (ISMS), conducting risk assessments across the company, and ensuring that identified risks are effectively managed to strengthen the company's overall risk posture. The department also supports Management in defining risk appetite and implementing appropriate controls to safeguard critical information assets.

- HR: HR is responsible for ensuring correct and appropriate screening of employees and on- and offboarding processes.

3.2. 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 utilises two different risk methodologies. Initially, ISO 27001 risk assessments are based on the implementation guidelines in ISO 31010 and ISO 27005 subsequently following an Octave approach.

Secondly, a customised approach for assessing risks related to software vulnerabilities has been implemented across the organisation. 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 ISO 31010 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 organisation, 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.

3.3. Control environment

The determination for establishing the control environment is based on ISO 27001:2022 – Annex A, referenced in ISO 27002. Unit IT is ISO 27001-certified, ensuring a structured approach to risk management across the four control domains: organisational, personnel-related, physical and technological controls. The certificate is available on 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:

- Organisational controls
- People controls
- Physical controls
- Technological controls.

3.3.1. Organisational 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 subsupplier and subprocessor, an annual collection of ISAE or SOC reports from the subservice supplier's independent body.

- If applicable in accordance with the criticality of the subsupplier and subprocessor, an annual collection of their ISO 27001 certificate.

Unit IT 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:

- Organisational responsibility to assess and monitor Unit IT's capabilities.

- Applicable laws and regulations have been identified.

- Privacy and PII have 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 independent reviews annually by an independent body.

3.3.2. 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, emphasising 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 organisational responsibilities.

3.3.3. Physical controls

Unit IT has implemented comprehensive physical and organisational controls to ensure the security and resilience of its hosting and housing facilities. Access to these facilities is strictly restricted to authorised 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 unauthorised access.

To reduce environmental risks, the facilities are equipped with advanced protection 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.

3.3.4. Technological controls

Access management

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 complex requirements. Unit IT has gradually transitioned to a state of a passwordless configuration to minimise 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 unauthorised 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 Defense 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.

Access to customer data and systems

Unit IT has implemented a service delivery platform that serves as the dedicated gateway for a limited number of employees to access customer data and systems where applicable. Access to the service delivery platform is conditional upon the fulfilment of specified security measures, which must be complied with to obtain such access. It is a prerequisite that the employee initially accesses the system from an approved device and only after using multi-factor authentication.

When these conditions have been met, the employee can request access to the service delivery platform. Hereafter, a request for access can be approved by a system owner if the employee has a work-related need.

Once access has been approved, a T-account is provisioned with a one-time token and remains valid only for a limited period. The T-account is automatically revoked upon expiry, and all activity is logged for both regular accounts and T-accounts.

Access is provided virtually, for example through Citrix, thereby ensuring that the employee's PC does not obtain direct access to any customer environment.

The service delivery platform does not share an Active Directory with Unit IT. The platform consists of several independent Active Directories, which are segregated from one another to ensure a higher level of security. The service delivery platform is monitored by Unit IT's 24/7 Cyber Defense Center.

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 Unit IT, 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 centralised 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.

3.4. Significant changes

The acquisition and establishment of our new office in Czech Republic, as described in section 3.1, is part of a strategy to transform and strengthen Unit IT as a managed services provider and provider of a wide range of services to private and public customers.

As part of the strategic initiatives, Unit IT has implemented significant organisational changes to enhance efficiency and alignment. Unit IT has implemented a new IT service management (ITSM) system to support organisational operations across the entire organisation and improve the management of customer requests and communication. Furthermore, Unit IT has implemented a new ERP system and a GRC system to support the management and maintenance of the information security management system (ISMS). Unit It's Cyber Defense Center has implemented a new AI-supported security operations platform, XSIAM, to support centralisation of data and automation of threat detection. We have continuously worked to further strengthen, standardise and formalise our key processes across the organisation to ensure greater consistency and efficiency.

Unit IT Holding A/S has successfully completed a robust consolidation of its three entities to strengthen alignment and operational efficiency to enhance the service we provide to our customers.

Please refer to section 4 for further description of control objectives and controls.

3.5. Complementary controls at the 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 covers all critical systems and communicate to Unit IT which systems need to be disaster recovery-tested and the frequency of such tests.

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 operating effectiveness 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 2025 to 31 December 2025. 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 included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

4.3.

4.4. Overview of control objectives, control activity, tests and test results

Control objective 4: Policy for risk assessment

- Formalised policies and procedures are established to ensure that roles, responsibilities and guidance are defined to support a structured process for identifying risks and integrating information security into the organisation.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
4.1	**Risk assessment and management** Risk assessments are conducted in accordance with ISO 27005 and ISO 31010, applying a structured methodology to ensure that risks are identified, assessed and communicated to Management for appropriate decision-making.	We inquired about the procedures/control activities performed. We inspected that formalised instruction in risk assessments is maintained.	No exceptions noted.
4.2	**Risk identification and analysis** The process ensures that risk assessments comprehensively address the following activities: • Risk identification: Systematically identify, document and describe potential risks relevant to the organisation's operations and objectives. • Risk analysis: Assess each identified risk by determining its root cause, likelihood of occurrence, potential impact and overall severity, providing a basis for Management decision-making and risk mitigation measures.	We inquired about the procedures/control activities performed. We inspected that risk identification and risk analysis have been performed.	No exceptions noted.
4.3	**Impact assessment** Impact analyses are conducted to evaluate the potential consequences of disruptions, considering the severity of damage to the organisation, with a specific focus on the loss of availability of information and essential services.	We inquired about the procedures/control activities performed. We inspected that impact analyses have been performed.	No exceptions noted.

Control objective 4: Policy for risk assessment

- Formalised policies and procedures are established to ensure that roles, responsibilities and guidance are defined to support a structured process for identifying risks and integrating information security into the organisation.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
4.4	**Standardised risk approach** All relevant stakeholders consistently apply a standardised risk assessment approach across all organisational units and departments to ensure uniformity, comparability and reliability in the evaluation of risks.	We inquired about the procedures/control activities performed. We inspected that risk assessments are standardised across all organisational units and departments.	No exceptions noted.
4.5	**Continuous risk assessment** The organisation ensures that the risk assessment and risk treatment measures are reviewed and updated continuously, at least annually and whenever significant changes affecting risks occur.	We inquired about the procedures/control activities performed. We inspected that risk assessment and risk treatment measures are reviewed and updated continuously, at least annually and whenever significant changes affecting risks occur.	No exceptions noted.
4.6	**Risk criteria** The organisation defines risk criteria and tolerance levels, obtains Management approval and communicates them to all relevant stakeholders.	We inquired about the procedures/control activities performed. We inspected that risk criteria and tolerance levels are approved by Management and communicated to relevant stakeholders.	No exceptions noted.
4.7	**Ongoing risk monitoring** Management regularly monitors identified risks, evaluates the progress and effectiveness of mitigation measures, and reviews changes in the overall threat landscape to support timely decision-making and ensure effective risk management.	We inquired about the procedures/control activities performed. We inspected that Management regularly monitors identified risks and evaluates the progress and effectiveness of mitigation measures.	No exceptions noted.

Control objective 4: Policy for risk assessment

- Formalised policies and procedures are established to ensure that roles, responsibilities and guidance are defined to support a structured process for identifying risks and integrating information security into the organisation.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
4.8	**Risk response activities** Following the annual risk assessment, Management evaluates whether updates to procedures or the implementation of compensating procedures are required to address identified risks, ensuring the organisation maintains an appropriate control environment.	We inquired about the procedures/control activities performed. We inspected that Management evaluates whether updates to procedures or the implementation of compensating procedures are required to address identified risks.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT'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 inquired about the procedures/control activities performed. We inspected that a Management-approved and updated security policy is in place. We 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 organisation needs.* Unit IT has defined and documented a policy for information security governance. This policy is to set out the governance of information security	We inquired about the procedures/control activities performed. By inspection, we observed that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	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.		
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 lines 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.	We inquired about the procedures/control activities performed. By inspection of random samples, we 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 organisation.*	We inquired about the procedures/control activities performed. We inspected that the information security policies are communicated to employees and relevant parties.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	Unit IT's Management has the overall responsibility for information security and for ensuring that all personnel are aware of and fulfil their information security responsibilities.		
5.7	**Threat intelligence** *Information relating to information security threats should be collected and analysed to produce threat intelligence.* Unit IT collects information security threats through recognised threat intelligence providers that provide the necessary intelligence for our monitoring platform.	We inquired about the procedures/control activities performed. By inspection, we 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 maintains inventories of all internal critical assets. Critical assets are assigned ownership and criticality. The criticality is reassessed annually by the asset owner. Unit IT has implemented multiple CMDBs for both internal and customers assets, depending on	We inquired about the procedures/control activities performed. We inspected that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	the assets in scope. This includes, but is not limited to, servers, networking equipment, databases, PCs, laptops and mobile devices.		
5.10	**Acceptable use of information and associated assets** *Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.* Unit IT has established, documented and implemented rules governing the acceptable use of information and associated assets, including hardware, software, networks, storage media and communication services.	We inquired about the procedures/control activities performed. We inspected that Unit IT has established and communicated an acceptable use policy.	No exceptions noted.
5.11	**Return of assets** *Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.* Unit IT has established appropriate processes to ensure that employees return their assets upon change or termination of their employment.	We inquired about the procedures/control activities performed. Checked by way of inspection of employees who have resigned or been dismissed during the assurance period that assets have been returned.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
5.12	**Classification** *Information should be classified according to the information security needs of the organisation based* on confidentiality, integrity, availability and relevant interested party requirements. Unit IT has a policy for data classification. Classification categories are documented, communicated to users and applied to applicable information to ensure appropriate protection and handling of information throughout its lifecycle.	We inquired about the procedures/control activities performed. We inspected that a policy for data classification has been implemented, reviewed and approved.	No exceptions noted.
5.15.1	**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 principle and users are only granted access based on a work-related need. Processes for access provisioning, access review and access revoking have been implemented for users managed by Unit IT.	We inquired about the procedures/control activities performed. We inspected that guidelines on access controls have been implemented, reviewed and approved.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
5.15.2	**Access control** *(customer-specific)* *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 defined rules to control access to customer installations. Unit IT has implemented a service delivery platform to access customer data. The service delivery platform is segregated from Unit IT's normal business operation and based on a tiering model.	We inquired about the procedures/control activities performed. We inspected that an access control policy and defined rules to control access to customer installations are implemented. We observed that a service delivery platform that is segregated from Unit IT's normal business network is utilised.	We noted that there is no formal procedure for access control in relation to customers' environments. In addition we noted that the process to some extent depends on one person. No further exceptions noted.
5.16.1	**Identity management** *The full life cycle of identities should be managed.* Unit IT has established processes to ensure that identification of individuals is managed appropriately. Access to Unit IT information systems is only allowed after provision of a unique user ID and password.	We inquired about the procedures/control activities performed. We inspected that procedures include the full life cycle of an identity.	No exceptions noted.
5.16.2	**Identity management** *(customer-specific)* *The full life cycle of identities should be managed.* Unit IT manages the full life cycle of identities within the service delivery platform. Access is	We inquired about the procedures/control activities performed.	We noted that there is no formal procedure for access control in relation to customers' environments. In addition we noted that the process to some extent depends on one person.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	granted only to authorised employees using approved devices and protected through multi-factor authentication (MFA). Access rights are automatically revoked after a defined period ensuring that access that is no longer required is removed.	Using samples, we inspected that access to the service delivery platform is only granted to authorised employees. We inspected that accounts are removed from customers' systems after a defined period.	No further exceptions noted.
5.17.1	**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 formalised 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).	We inquired about the procedures/control activities performed. By inspection, we observed that Unit IT has established formalised procedures for user administration and rights management. We observed that authorisations granted at Unit IT include an access request justification.	No exceptions noted.
5.17.2	**Authentication information** *(customer-specific)* *Allocation and management of authentication information should be controlled by a management*	We inquired about the procedures/control activities performed. We observed that MFA is utilised to access the service delivery platform.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	process, including advising personnel on the appropriate handling of authentication information. Access to the service delivery platform is restricted to authorised employees using approved devices and safeguarded through MFA.		
5.18.1	**Access rights** *Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation'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 are performed according to Unit IT's policies. Unit IT follows a least privilege access principle, and users are only granted access based on a work-related need.	We inquired about the procedures/control activities performed. Checked by way of inspection of employees who have resigned or been dismissed during the assurance period that rights have been deactivated or terminated. Checked by way of inspection of a sample of users' access to systems and databases that such access is approved by a manager and restricted to the employees' work-related need. By inspection, we observed that user access rights are reassessed once every month.	No exceptions noted.
5.18.2	**Access rights** *(customer-specific)* *Access rights to information and other associated assets should be provisioned, reviewed, modified*	We inquired about the procedures/control activities performed. By inspection, we observed that user access rights are reassessed once every six months.	We noted that there is not sufficient documentation of periodic review of privileged access rights in relation to customers' environments. No further exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	and removed in accordance with the organisation's topic-specific policy on and rules for access control. Unit IT has implemented a service delivery platform that serves as the dedicated gateway for a limited number of employees to access customer data and systems where applicable. It is a prerequisite that the employee initially accesses the system from an approved device and only after using MFA. Hereafter, a request for access can be approved by a system owner if the employee has a work-related need.	Using samples, we inspected that access to the service delivery platform is only granted to authorised employees.	
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 suppliers' 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.	We 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.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	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.		
5.20	**Addressing information security within supplier agreements** *Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.* Unit IT has established information security requirements for suppliers based on their criticality. Each supplier is assessed on their criticality for Unit IT's core business processes. The criticality is reassessed upon any major changes in the agreement with the supplier or at Unit IT.	We inquired about the procedures/control activities performed. We inspected that suppliers are assessed on the basis of their criticality.	No exceptions noted.
5.22	**Monitoring, review and change management of supplier services** *The organisation 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	We inquired about the procedures/control activities performed. We 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.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	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.	From a sample of signed contracts, we observed that information security requirements have been contractually agreed. We observed that Unit IT audits key suppliers on a periodic basis, based on agreed information security requirements. We observed that third-party assurance reports have been received and processed by Unit IT for key suppliers.	
5.24	**Information security incident management responsibilities and preparation** *The organisation 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 have been clearly defined and communicated to all relevant employees.	We inquired about the procedures/control activities performed. We observed that a formal and documented incident management process related to information security events and breaches has been implemented. We observed that the incident management processes have been communicated to employees. We observed that incidents are registered, that necessary actions are performed and that the solutions are documented in an incident management system and reported through the Information Security Board.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
5.25	**Assessment and decision on information security events** *The organisation should assess information security events and decide if they are to be categorised as information security incidents.* All internal information security events are logged, assessed and evaluated to determine their impact, and a decision is made as to whether they should be categorised and handled as information security incidents.	We inquired about the procedures/control activities performed. We observed that a formal and documented incident management process related to information security events and breaches has been implemented. We inspected that internal security incidents are evaluated and categorised.	No exceptions noted.
5.26	**Response to information security incidents** *The organisation should assess information security events and decide if they are to be categorised as information security incidents.* Information security incidents within Unit IT are efficiently and effectively managed by designated employees with the required competencies.	We inquired about the procedures/control activities performed. We observed that a formal and documented incident management process related to information security events and breaches has been implemented.	No exceptions noted.
5.29	**Information security during disruption** *The organisation 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 se-	We inquired about the procedures/control activities performed. We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually.	We noted that the business continuity plan has not been updated or approved since 2022. No further exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure Management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems is managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and ensure correct and secure operation of information processing facilities.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
	curity 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 inspected that a business impact assessment has been performed to establish the requirements of a business continuity plan. We inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	
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 inquired about the procedures/control activities performed. We inspected that operating procedures have been established and that these are subject to updating at least once a year. We inspected that the operating procedures are accessible to all relevant employees.	No exceptions noted.

Control objective 6: People controls

- Procedures and controls ensure that background checks are conducted, security requirements are included in contracts, training is provided, disciplinary actions are enforced and security responsibilities are managed post-employment.
- Procedures and controls ensure the use of confidentiality agreements, secure remote work arrangements and prompt reporting of security events.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
6.1	**Screening** *Background verification checks on all candidates should be carried out prior to joining the organisation 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 inquired about the procedures/control activities performed. We inspected that an HR process is in place to ensure that criminal records are presented before start of employment for both employees and external consultants. Using samples, we inspected that criminal records have been acquired before start of employment for new hires.	No exceptions noted.
6.2	**Terms and conditions of employment** *The employment contractual agreements should state the personnel's and the organisation's responsibilities for information security.* Responsibilities for information security are clearly defined in all employment contracts between the company and the employee.	We inquired about the procedures/control activities performed. Using random samples, we inspected that responsibilities for information security are clearly defined in employment contracts.	No exceptions noted.

Penneo dokumentnøgle: AW7D8-0HYYX-0E5U4-55YFV-EZL05-9SGW9

Control objective 6: People controls

- Procedures and controls ensure that background checks are conducted, security requirements are included in contracts, training is provided, disciplinary actions are enforced and security responsibilities are managed post-employment.
- Procedures and controls ensure the use of confidentiality agreements, secure remote work arrangements and prompt reporting of security events.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
6.3	**Information security awareness, education and training** *Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation'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 inquired about the procedures/control activities performed. We observed that Unit IT runs introductory courses for new employees during which information security requirements are explained. We 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.
6.4	**Disciplinary process** *A disciplinary process should be formalised and communicated to take action against personnel and other relevant interested parties who have committed an information security policy violation.* Unit IT has communicated to all employees that the failure to comply with information security instructions may have consequences for their employment at Unit IT.	We inquired about the procedures/control activities performed. We inspected that employees appointed during the assurance period have signed a contract in which it is stated that failure to comply with information security instructions may have consequences for their employment at Unit IT.	No exceptions noted.

Control objective 6: People controls

- Procedures and controls ensure that background checks are conducted, security requirements are included in contracts, training is provided, disciplinary actions are enforced and security responsibilities are managed post-employment.
- Procedures and controls ensure the use of confidentiality agreements, secure remote work arrangements and prompt reporting of security events.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
6.5	**Responsibilities after termination or change of employment** *Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.* All employees are informed of the information security responsibilities and duties after their employment at Unit IT. This is communicated in all employee contracts upon employment.	We inquired about the procedures/control activities performed. We inspected that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We inspected for employees who have resigned or been dismissed during the assurance period that documentation confirms the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
6.6	**Confidentiality or non-disclosure agreements** *Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.* Confidentiality agreements are signed by all employees upon employment at Unit IT.	We inquired about the procedures/control activities performed. We inspected that employees appointed during the assurance period have signed a confidentiality agreement.	No exceptions noted.

Control objective 7: Physical controls

- Procedures and controls ensure the establishment and maintainance of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Unit IT'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. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected the physical security controls at the facilities. We 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.
7.2	**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. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected the physical security controls at the facilities. We observed that Unit IT has implemented appropriate entry controls to protect physical facilities. We 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.

Control objective 7: Physical controls

- Procedures and controls ensure the establishment and maintainance of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
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 process sensitive information. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. We inspected the physical security controls at the facilities. We observed that Unit IT has implemented appropriate entry controls to protect physical facilities. We 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.
7.4	**Physical security monitoring** *Premises should be continuously monitored for unauthorised physical access.* Unit IT has established access controls to data centres to prevent and detect unauthorised physical access to the premises. Unit IT has installed video monitoring systems in all critical data centres. Data centres are monitored 24/7 365. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. We inspected the physical security controls at the facilities. We 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.

Control objective 7: Physical controls

- Procedures and controls ensure the establishment and maintainance of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
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 process sensitive information to protect against physical and environmental threats. Appropriate internal controls have been implemented to mitigate risks of potential physical and environmental threats. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. We inspected the physical security controls at the facilities. We 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 data centres to prevent and detect unauthorised physical access or suspicious behaviour. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. We 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.

Control objective 7: Physical controls

- Procedures and controls ensure the establishment and maintainance of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Unit IT'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 and fibers) are containerised in the quest for resiliency. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. We observed that Unit IT has implemented appropriate controls to protect physical facilities and cabling security. We 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.
7.13	**Equipment maintenance** *Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.* Equipment is maintained according to procedures to ensure availability, integrity and confidentiality of information. Maintenance records were reviewed and found to be complete and up to date. Unit IT has obtained an audit report from a subcontractor and has viewed the audit report to ensure that similar requirements are met in areas subject to outsourcing.	We inquired about the procedures/control activities performed. We 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.

Control objective 7: Physical controls

- Procedures and controls ensure the establishment and maintainance of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
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 media are disposed of through a certified supplier.	We inquired about the procedures/control activities performed. We inspected that Unit IT has implemented procedures on secure disposal or re-use of equipment. We 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

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT'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 include 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 inquired about the procedures/control activities performed. We observed that all types of identified assets, including endpoint devices, are listed in the acceptable use policy. We observed that updates to the acceptable use policy are communicated to employees. We observed that a process is in place to maintain an approved whitelist of allowed services and applications.	No exceptions noted.
8.2.1	**Privileged access rights** *(customer-specific)* *The allocation and use of privileged access rights should be restricted and managed.* Privileged access is defined in Unit IT'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 inquired about the procedures/control activities performed. We 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 inspected that authorisation granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior.	We noted that there is no formal procedure for access control in relation to privileged access to infrastructure supporting customers' environments; hence we were not able to sample test approval of access. No further exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
8.5.1	**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 MFA.	We inquired about the procedures/control activities performed. We inspected that a formal policy for access control that defines allowed technical solutions for authentication is maintained. Using samples, we inspected that the user registration and de-registration process has been implemented.	No exceptions noted.
8.5.2	**Secure authentication** *(customer-specific)* *Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.* Unit IT has implemented secure authentication technologies for accessing customer data, incorporating MFA and ensuring that access is only possible from secure, company-approved devices.	We inquired about the procedures/control activities performed. We observed that MFA is utilised to access to the service delivery platform.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
8.7	**Protection against malware** *Protection against malware should be implemented and supported by appropriate user awareness.* All Unit IT endpoint devices have enhanced malware protection, detection and remediation enabled. Disabling any type of protection automatically alarms Unit IT's CDC, and the device is subsequently denied access to processing facilities. According to the individual customer contract, Unit IT deploys anti-malware on hosted servers.	We inquired about the procedures/control activities performed. We inspected that the employees' computers managed by Unit IT are protected by antivirus 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 organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.* Unit IT has established an instruction to assess technical vulnerabilities in order to identify security weaknesses, evaluate the potential impact and mitigate the impact of vulnerabilities.	We inquired about the procedures/control activities performed. We inspected that there is a formal procedure for risk assessing vulnerabilities.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
8.10	**Information deletion** *Information stored in information systems, devices or any other storage media should be deleted when no longer required.* Customer information and data are handled and deleted in accordance with contractual obligations.	We inquired about the procedures/control activities performed. Using samples, we inspected that data relating to terminated customer relationships have been deleted in accordance with the applicable retention periods.	No exceptions noted.
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.* Unit IT performs daily backups and regular restore tests of business-critical systems. In accordance with customer contracts, backup jobs are monitored to ensure continuous operation. All backup data are kept isolated from the processing data centres. Restores of customer backups are tested in accordance with customer contracts.	We inquired about the procedures/control activities performed. Using samples, we inspected that daily backup jobs are performed. We inspected that failed backup job are handled and logged. We inspected an architectural drawing of the backup environment. We inspected that restore tests of customers' IT environments are performed upon request.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT’s control activity	Tests performed by PwC	Result of PwC’s tests
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 automatic 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 data centres.	We inquired about the procedures/control activities performed. We observed that key operating areas have been outsourced to a supplier. We observed that Unit IT follows up on delivered services from suppliers. We inspected data processing facilities and systems. We observed that within the systems redundant and failover capabilities for servers, network and storage are implemented.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT'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 has been implemented to protect log information. Users with access to log information do not have access to source systems.	We inquired about the procedures/control activities performed. We 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 inquired about the procedures/control activities performed. Using samples, we inspected that logging parameters are set up to ensure that actions performed by users with extended access rights are logged.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
8.17	**Clock synchronisation** *The clocks of information processing systems used by the organisation should be synchronised to approved time sources.* Unit IT has synchronised all relevant information processing systems to a single reference time source.	We inspected the system configuration for network time synchronisation. We observed that an NTP has been configured. On a sample basis, we inspected the clock configuration.	No exceptions noted.
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 data centres are secured via encrypted network tunnels. All changes to the configuration of the network or security measures must be tested, approved and documented according to the generally applicable change management process.	We inquired about the procedures/control activities performed. We inspected system configurations for firewall, network switches and network topology. We observed that the network is protected with firewalls and segregated. Using samples, we inspected that the change management procedure is followed.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT's control activity	Tests performed by PwC	Result of PwC's tests
8.22	**Segregation in networks** *Groups of information services, users and information systems should be segregated in the organisation'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 inquired about the procedures/control activities performed. We inspected system configurations for firewall, network switches and network topology. We 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 inquired about the procedures/control activities performed. We inspected that rules for appropriate use of secure cryptography and key management have been established.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures, and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity. Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Unit IT'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 inquired about the procedures/control activities performed. We inspected the adequacy of change management procedures and inspected that an appropriate change management system is established supported by a technical infrastructure. We inspected that a formal change management procedure has been implemented in the organisation. Using samples, we inspected that the change management procedure is followed.	No exceptions noted.

PENNEO

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
CEO
På vegne af: Unit IT Holding A/S
Serienummer: c51d4162-810e-4a38-8c1b-2deada7381a0
IP: 93.176.xxx.xxx
2026-02-05 07:41:36 UTC

Mit ID ✓

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-02-05 08:04:16 UTC

Mit ID ✓

Rico Lundager
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Director
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 2e75390a-f48a-4123-b26c-3fd3e97823aa
IP: 83.136.xxx.xxx
2026-02-05 10:09:25 UTC

Mit ID ✓

Penneo dokumentnøgle: AW7D8-0HYYX-0E5U4-55YFV-EZL05-95GW9

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se **https://eutl.penneo.com**.

Sådan kan du verificere, at dokumentet er originalt
Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskriveres digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, **https://penneo.com/validator**, eller andre valideringstjenester for digitale underskrifter.