itm8 A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2024 to 31 December 2024 in relation to itm8's hosting services

February 2025

Contents

1 Management's statement 3

2 Independent service auditor's assurance report on the description, design and operating effectiveness of controls 5

3 Service organisation's system description 8

4 Control objectives, control activity, tests and test results 17

1 Management's statement

The accompanying description has been prepared for customers who have used itm8 A/S's hosting services 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 the customers' financial statements.

itm8 A/S uses Fuzion and InterXion as subservice suppliers for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that Fuzion and InterXion perform for itm8 A/S.

itm8 A/S uses B4Restore and Keepit as subservice suppliers for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore and Keepit perform for itm8 A/S.

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

itm8 A/S confirms that:

a) The accompanying description in section 3 fairly presents the hosting services that have processed customers' transactions throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

(iii) Presents how IT general controls in relation to the hosting services 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 hosting services, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
- How the system dealt with significant events and conditions other than transactions
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the IT general controls

(ii) Includes relevant details of changes to IT general controls in relation to the hosting services during the period from 1 January 2024 to 31 December 2024

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

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

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

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

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

Herning, 3rd February 2025
itm8 A/S

Frank Bech Jensen
Head of Compliance and Security

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2024 to 31 December 2024 in relation to itm8's hosting services

To: itm8 A/S (itm8), itm8's customers and their auditors

Scope

We have been engaged to provide assurance about itm8's description in section 3 of its IT general controls in relation to its hosting services which have processed customers' transactions throughout the period from 1 January 2024 to 31 December 2024 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

itm8 uses Fuzion and InterXion as subservice suppliers for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that Fuzion and InterXion perform for itm8.

itm8 uses B4Restore and Keepit as subservice suppliers for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore and Keepit perform for itm8.

Some of the control objectives stated in itm8's description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with itm8's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

itm8's responsibilities

itm8 is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on itm8's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its hosting services and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by itm8 in the Management's statement section.

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

Limitations of controls at a service organisation

itm8'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 hosting services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

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

a) The description fairly presents how IT general controls in relation to the hosting services were designed and implemented throughout the period from 1 January 2024 to 31 December 2024;

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

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

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used itm8's hosting services and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Aarhus, 3rd February 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen State-Authorised Public Accountant mne26801	Iraj Bastar Director

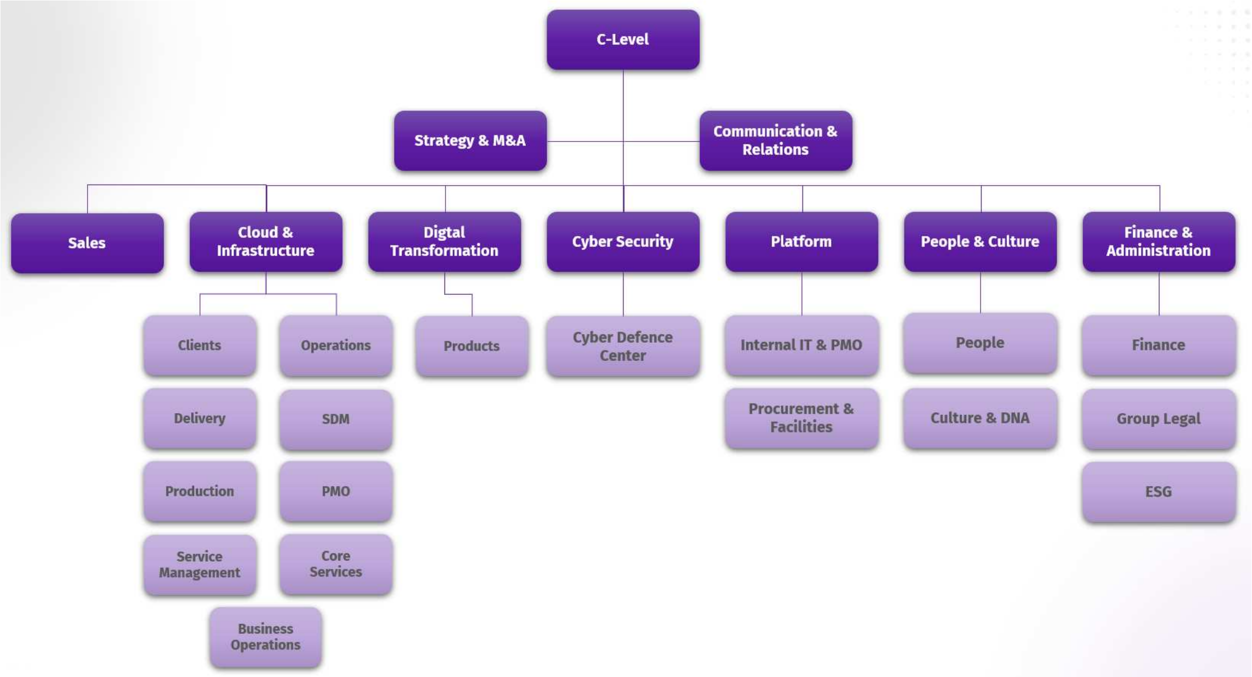
3 Service organisation's system description

Description of the service organisation

itm8 A/S has undergone rapid development to become a structured organisation delivering specialised IT services and solutions. itm8 is organised into several divisions, including both customer-facing divisions that drive service delivery and business divisions that provide essential administrative and operational support. This setup enables itm8 to offer integrated, reliable services that meet high standards of quality and compliance for a diverse client base.

This independent assurance report is focused on itm8 | Cloud & Infrastructure, which is included as the scope of this report. The division provides cloud solutions and IT infrastructure services that align with itm8's standards for quality and secure service delivery. Additionally, the scope includes specific components from itm8 | Cybersecurity, particularly the Cyber Defence Center, which delivers 24/7 monitoring, SIEM log management and incident response essential to infrastructure security.

Further, the report includes elements of itm8 | Digital Transformation, specifically the Team Products group, which develops custom solutions such as Send Secure (SEPO) and the Dental Records system (TK2). These specialised solutions support itm8's commitment to secure, tailored services that meet clients' unique operational needs.



Scope of the itm8 | Cloud & Infrastructure independent assurance report

Customer divisions

The customer-facing divisions are itm8's primary service pillars, each dedicated to specific areas of expertise:

- itm8 | Cloud & Infrastructure
  Focused on cloud solutions and IT infrastructure, this division helps customers implement robust hosting and operational strategies. It transforms client business strategies into scalable cloud and

infrastructure solutions through platform assessments, security policy design, migrations, modernisation and 24/7 support.

- itm8 | Cybersecurity
  Offering comprehensive security services, itm8 | Cybersecurity spans everything from penetration testing and red teaming to cyber risk consultancy. It includes a Cyber Defence Center for continuous SIEM log management, vulnerability assessments and real-time incident response.

- itm8 | Digital Transformation
  This division drives digital innovation for clients, offering ERP integration, SharePoint and Microsoft solutions, along with unique products developed by Team Products, such as the Send Secure platform and Dental Records system (TK2), to optimise business processes.

- itm8 | Application Services
  itm8's Application Services division accelerates application development and maintenance with a focus on security and quality. Services include application management, database administration, monitoring, performance tuning and technical support.

Business divisions

Supporting these pillars, itm8's business divisions – such as HR, Marketing, Legal, Internal IT and Compliance & Security – provide the foundation for effective service delivery. These divisions are integral to itm8's operational integrity and ensure that all customer-facing activities align with itm8's standards and regulatory requirements.

Together, these divisions create a robust structure that enables itm8 to deliver specialised, high-quality services aligned with clients' strategic goals.

Information security management system

The information security management system (ISMS) at itm8 | Cloud & Infrastructure is designed to align seamlessly with the requirements of ISO 27001:2022, embedding information security into our organisational processes and culture.

Context of the organisation

Our ISMS is tailored to the context of itm8, considering our strategic objectives, external and internal challenges and the needs and expectations of our stakeholders. Through stakeholder analysis, we ensure that our information security measures are aligned with the expectations of interested parties and responsive to the evolving risk landscape.

Leadership

Leadership commitment is a cornerstone of our ISMS. Top Management has defined and approved a robust information security policy that establishes the organisation's security goals and ensures alignment with overall business objectives. Leadership is also actively involved in fostering a culture of security, ensuring that adequate resources are allocated and that roles and responsibilities are clearly communicated and understood throughout the organisation.

Planning

The planning aspect of our ISMS is grounded in a structured risk management process and methodology, supported by a dedicated system. We conduct regular risk assessments to identify, evaluate and mitigate risks, ensuring they are managed within acceptable levels. Information security objectives are established, periodically reviewed and integrated into the company's broader strategic planning, ensuring a proactive approach to managing information security risks.

Support

Our ISMS is supported by a document management system (DMS) that securely stores all official documentation and meets quality requirements. We also maintain a comprehensive security awareness programme that provides continuous training and testing to ensure all employees understand their roles in maintaining and enhancing information security. This programme focuses on ongoing competence development and awareness across the organisation.

Operation

We implement and manage our processes based on the ITIL framework, ensuring that all operations are consistent with best practices and our defined information security objectives. Our operational approach integrates security considerations into daily business activities, embedding security into the organisational fabric. The DMS serves as a central repository for all processes, procedures and policies, ensuring that all operational activities are carried out in alignment with the ISMS.

Performance evaluation

The ensure the effectiveness of our ISMS, we regularly monitor, measure and evaluate our information security processes. This includes a structured internal audit programme that systematically reviews all elements of the ISMS over a three-year cycle. These audits, along with management reviews and other performance metrics, provide critical insights that help us maintain alignment with evolving business needs and emerging threats. The findings from these evaluations are used to drive continuous improvement and ensure that our ISMS remains effective and up-to-date.

Improvement

Continuous improvement is embedded in our ISMS through bi-monthly Continuous Improvement Meetings (CIM) within the Compliance & Security team. These meetings, officially recorded with drafted minutes, provide a forum to discuss all aspects information security across itm8. Insights from these discussions, along with findings from our internal audits and performance evaluations, are used to drive improvements in our ISMS. We are committed to a cycle of continual enhancement, ensuring that our ISMS remains dynamic and effective in addressing emerging threats and aligning with industry best practices.

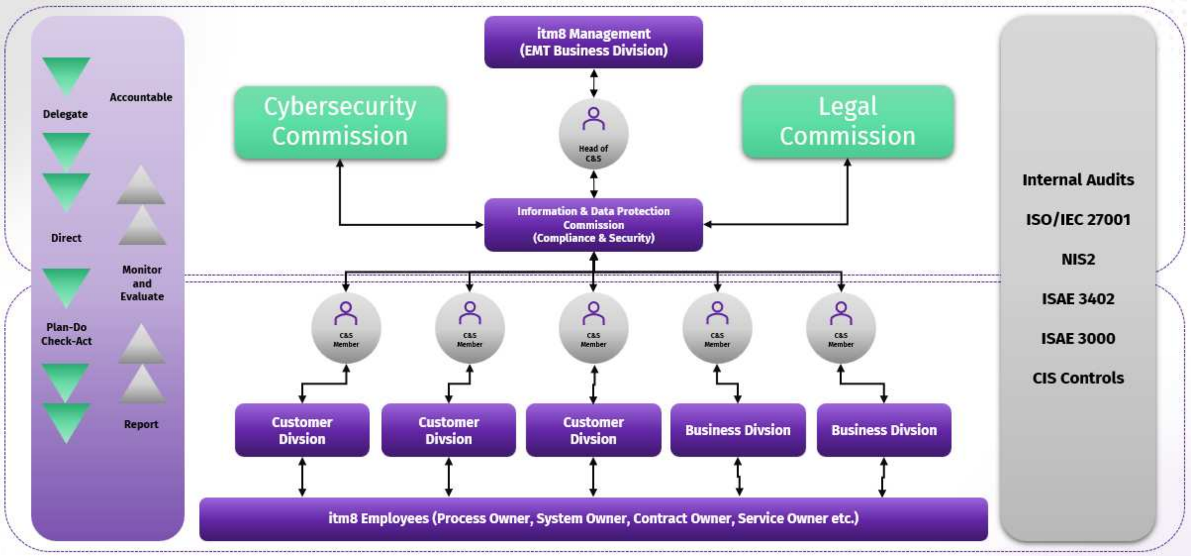
There have been no significant changes to procedures and controls in the period from 1 January 2024 to 31 December 2024.

Information security governance

Information security governance at itm8 | Cloud & Infrastructure is designed to ensure that security practices are embedded across the organisation, in alignment with ISO/IEC 27001:2022. Our approach begins with an information security policy, approved by Top Management, which outlines our security objectives and is supported by 15 topic-specific policies. These policies cover areas such as access control, asset management, business continuity and incident management, and are owned by the Compliance and Security team, with relevant policies communicated to specific stakeholders.

We have clearly defined information security roles, including positions like information security manager, system owner, and process owner, to ensure that responsibilities are clearly assigned and understood. Segregation of duties is implemented in critical functions such as backup, finance, change management and development to mitigate risks associated with unauthorised access or errors.

Our information security governance structure assigns overall responsibility to Top Management, who delegate to the Compliance & Security team. This team collaborates with the Cybersecurity and Legal Commissions to address technical and legal security aspects. Compliance & Security team members are aligned with specific divisions, working with roles like process owners, system owners, and services owners to implement security measures throughout itm8.



itm8 security governance structure

Management plays a crucial role in supporting our information security framework, ensuring compliance with applicable requirements and actively engaging in the governance of our ISMS. We maintain an updated list of all relevant authorities and legislation, completed with assigned owners, to ensure compliance and facilitate communication with regulatory bodies. Our involvement in various special interest groups, such as security forums and IT networking groups, keeps us informed about industry trends and best practices.

Information security is also integrated into our project management practices through a risk management process, requiring project managers to conduct a preliminary risk analysis at the start of a project. This ensures that security considerations are addressed early in the project lifecycle, further embedding information security into our organisational processes and culture.

Asset management

itm8 | Cloud & Infrastructure manages its information and associated assets according to ISO/IEC 27001:2022 standards. We maintain asset inventories using various databases, including a primary CMDB for CI's and customer facing solutions and InTune MDM for endpoint management. Clear policies and security one-pagers outline acceptable use, ensuring all employees understand how to handle assets responsibly.

Asset return procedures are built into our HR processes, ensuring secure returns when employees leave or change roles. We have established guidelines for securing assets off-site, as well as handling storage media on both endpoint devices and customer-facing platforms like servers.

Procedures are in place for the secure disposal and reuse of equipment, covering both internal and customer-facing assets, ensuring that all data is properly erased. User endpoint devices are centrally managed and domain-joined, allowing us to enforce security configurations and maintain control over these assets.

Information protection

At itm8 | Cloud & Infrastructure, we ensure robust information protection in line with ISO/IEC 27001:2022 controls. We have established a classification scheme detailed in our Principles & Rules for Information Protection, which guides the classification and labelling of information according to its sensitivity. This helps ensure that all information is handled appropriately based on its classification.

To protect data during transfer, we have developed specific rules and policies, including security one-pagers, that outline secure methods for information exchange. Protection of records is managed through default system design and established procedures, with a strong focus on maintaining privacy and compliance with the EU GDPR for Personally Identifiable Information (PII).

We have established clear procedures for information deletion to ensure data is securely removed when no longer needed. Data masking techniques are applied when using test data sourced from production environments, maintaining privacy and security even in testing scenarios.

To prevent data leakage, we have implemented monitoring activities designed to detect and mitigate any unauthorised data exposure. Test information is protected according to our establishes standards and relevant agreements, ensuring it is handled with the same care as live data.

Human resource security

Human resource security at itm8 | Cloud & Infrastructure is managed in accordance with ISO/IEC 27001:2022 to ensure that all personnel are adequately vetted, training and held accountable for their roles in information security. We conduct employee screening upon recruitment, which includes obtaining a clean criminal record, and this check is repeated every three years of employment to maintain a high level of trustworthiness.

Our terms and conditions of employment include specific clauses related to information security, ensuring that all staff understand their obligations. We have a security awareness programme that involves regular training, continuous phishing simulations, and other testing scenarios to keep employees prepared for security threats.

To address breaches of information security, we have a disciplinary process in place which is applied when necessary to enforce our security policies. After termination or changes in employment, we manage access rights carefully, revoking or adjusting them as appropriate to maintain security.

Confidentiality and non-disclosure agreements are integral parts of our employment contracts, with additional agreements put in place for certain roles depending on customer requirements. For remote working, we have established specific rules and guidelines, detailed in our security one-pagers, to ensure that employees maintain security standards while working off-site.

Physical security

itm8 | Cloud & Infrastructure maintain robust physical security measures aligned with ISO/IEC 27001:2022 to protect our assets and facilities. Physical security perimeters are established at both office and data centre locations, defining areas that require protection and the specific security measures needed. Physical entry to these locations is controlled through the use of ID cards, PINs and alarm system at key entry points.

Offices, rooms and facilities are secured based on their sensitivity, with defined security zones that have tailored measures to protect against unauthorised access. We implement protections against physical and environmental threats, adjusting security controls according to the level of sensitivity of the information housed within a location.

Guidelines and procedures for working in secure areas are in place to maintain a high standard of security within these environments. A clear desk and clear screen policy is enforced, with expectations communicated through our security one-pagers to ensure sensitive information is not left exposed.

Equipment is sited and protected based on its sensitivity and purpose, with secure placements ensuring the safety and integrity of our hardware. Supporting utilities are tailored to the needs of each location; for instance, data centres and other critical sites are equipped with backup generators and UPS systems to maintain operations during power disruptions.

We also ensure that all equipment is professionally maintained according to manufacturer recommendations, ensuring that it operates effectively and remains secure throughout its lifecycle. Cabling is securely managed to prevent tampering and unauthorised access, and all equipment maintenance activities are performed to maintain the highest standards of operational security.

System and network security

System and network security at itm8 | Cloud & Infrastructure is managed in accordance with ISO/IEC 27001:2022 to ensure a secure operating environment for both internal and customer systems. We have established documented operating procedures that guide the handling of various tasks within our IT environments, ensuring consistency and security across all operations.

To protect against malware, we implement and monitor protection measures across our internal infrastructure and extend these services to customer environments as contracted. The use of privileged utility programs is restricted to a designated group of employees, ensuring that only authorised personnel have access to critical functions.

Our network security framework includes multiple layers of defence, such as DMZs, firewalls and segregated environments, tailored to protect both production and office networks. Network services are set up securely, following best practices and customer agreements, ensuring that services meet contractual and security requirements.

We maintain strict network segregation, with production and office networks kept separate, and customer networks segmented according to their specific agreements to maintain data integrity and security. Web filtering measures, including Safelinks, are in place to alert users to potentially malicious sites, and breaches of these safeguards trigger notifications to our Cyber Defense Center for immediate action.

Change management is an integral part of our approach, with a structured process that includes risk assessment of changes. Critical changes are reviewed at CAB meetings to ensure that potential impacts are fully evaluated and mitigated, maintaining the security and stability of our systems and networks.

Application security

itm8 | Cloud & Infrastructure manages application security in line with ISO/IEC 27001:2022 controls. Access to source code is restricted to employees who require it, ensuring sensitive code is protected. We have implemented a secure development life cycle that integrates security requirements tailored to the criticality of each application.

Secure system architecture and coding practices are followed to reduce vulnerabilities, and security testing is conducted during development and acceptance stage to validate applications before they are moved into production.

For outsourced development, specific guidelines ensure security standards are met.

Development, test and production environments are kept separate to prevent interference and maintain system integrity.

Secure configuration

We have a configuration management process supported by a centralised CMDB, which is used to manage all configuration items (CIs) for both internal systems and customer-facing environments.

Our patch management procedure ensures that software updates and patches are applied securely and in line with contractual agreements. Additionally, we have established rules governing the use of cryptography to protect data and communications, ensuring they meet required security standards.

Identity and access management

At itm8 | Cloud & Infrastructure, identity and access management adheres to ISO/IEC 27001:2022 controls to safeguard access to systems and information. We have implemented an access control policy and associated procedures to regulate access effectively.

Identity management is handled collaboratively by personnel management, User Management and Human Resources, covering the entire lifecycle of user identities. Authentication practices are defined for both customer-facing and internal environments, ensuring secure methods are in place.

Access rights are assigned based on job requirements, and we limit privileged access to essential personnel only. Specific rules govern the management of privileged accounts and authentication information. Access to sensitive information, including customer data and HR records, is restricted according to predefined policies.

Secure authentication is enforced, with multi-factor authentication (MFA) applied where critical to enhance security.

Threat and vulnerability management

Threat and vulnerability management is aligned with ISO/IEC 27001:2022 controls to protect our systems and data. We conduct threat intelligence at multiple levels; strategic, tactical and operational. Strategic threat intelligence addresses broader societal, geopolitical and market threats, while tactical and operational intelligence focuses on technical aspects such as specific vulnerabilities, attack patterns and malicious entities.

Out management of technical vulnerabilities is guided by a defined procedure. This including ongoing vulnerability assessments and management within our own internal environment, with responsibilities assigned to technology owners to ensure timely identification and remediation of vulnerabilities.

Continuity

Continuity management is designed to ensure ongoing operations and resilience. Our business continuity plans outline communication strategies, roles and procedures for maintaining business functions during disruptions or major incidents.

Capacity management is addressed through established criteria and thresholds, with ongoing monitoring of platform capacities to ensure timely adjustments and prevent potential issues.

We maintain comprehensive and secure backup facilities, including redundant backups managed by an ISO/IEC 27001-certified third-party supplier. These backups are stored in geolocated facilities separate from the original production environment to ensure their availability even during significant disruptions.

Supplier relationships security

At itm8 | Cloud & Infrastructure, we manage supplier relationships with a strong focus on information security. Our agreements with supplier often include security addendums, where possible and applicable, and we actively monitor supplier operations for potential issues.

A formal supplier onboarding procedure ensures that suppliers are categorised and evaluated before entering into agreements. We perform continuous risk assessments for critical suppliers to manage potential risks effectively.

Our cloud security strategy outlines the security considerations for cloud services, including strategies for managing and exiting cloud partnerships as needed, ensuring ongoing security throughout the lifecycle of these services.

Legal and compliance

We ensure adherence to legal, statutory, regulatory and contractual requirements by maintaining an overview of applicable obligations and assigning internal owners for each requirements.

Intellectual property rights (IPR) are protected through established rules and guidelines included in our policies and employee contracts, ensuring proper management and safeguarding of intellectual assets.

We conduct continuous independent review of our information security practices, including ISAE 3402 and ISAE 3000 audits for hosting services and data protection, as well as audits by customers and external audits in line with our ISO 27001 certification.

We remain compliant with relevant policies, rules and standards for information security, continuously updating our practices to align with various frameworks and ensuring our measures reflect current compliance requirements.

Information security event management

We manage information security events through a structured incident management process, including major incidents and security incidents procedures. These procedures detail roles, responsibilities and the steps for assessing, responding to and learning from incidents.

We ensure thorough evidence collection during incident management to support analysis and provide documentation for review. Information security events are continuously reported to Top Management as part of our regular management reviews, as well as reviewed during our bi-monthly Continuous Improvement Meetings.

Our SIEM log management solution logs and monitor activities around the clock, while clock synchronisation is maintained to ensure accurate time stamps for alerts, providing a reliable overview of events and IT environment operations.

Control objectives and activities are detailed in section 4.

Complementary controls at customers

Matters to be considered by customers' auditors

Services provided

The above system description of controls is based on itm8's standard terms. Customers' deviations from itm8's standard terms are therefore not covered by this statement. Customers' own auditors should therefore assess whether this statement can be extended to cover the specific customer and identify any other risks that are relevant to the presentation of customers' accounts. Regarding change management, only the core infrastructure is covered by the standard contracts, and any change management on customer solutions must be covered by a separate agreement with itm8.

User administration

itm8 assigns access and rights in accordance with the customer's instructions when these have been reported to the service desk. itm8 is not responsible for the accuracy of this information, and it is therefore the customers' responsibility to ensure that access and rights to systems and applications are assigned appropriately and in accordance with best practice for separation of duties. itm8 also grants access to third-party consultants – primarily developers who are to maintain applications included in the hosting agreement. This is done in accordance with instructions from itm8's customers. The customers' own auditors should therefore independently assess whether the access and rights to applications, servers and databases granted to the customer's own employees and to third-party consultants are appropriate based on an assessment of the risk of misstatements in the financial reporting. As standard, itm8 and the customer's internal IT employees use a common system access (common administrator password). The accounts used by itm8 are often accounts with extended rights. As an increased protection of these accounts, itm8 offers a Just-in-Time solution. This is not part of the standard contract with itm8. Just-in-Time is a system for protecting itm8's administrator accounts. This ensures that access usage is logged and traceable, that strong passwords are used, and that passwords are changed each time the account is used. With Just-in-Time, no one knows the password when itm8 is not logged in. This limits the possibility that an itm8 account can be used by a hacker for lateral movement, and that an employee can remember a password when he is no longer employed by IT itm8.

Contingency planning

The general terms and conditions for hosting at itm8 do not stipulate requirements for contingency planning and restoration of the customers' system environment in the event of an emergency. itm8 ensures general backup of the customer environments, but the hosting agreements do not include a guarantee for full restoration of the customers' system environment after an emergency. The customers' own auditors should therefore independently assess the risk of lack of contingency planning and regular testing thereof in relation to a risk of misstatement in the financial reporting.

Compliance with relevant legislation

itm8 has planned procedures and controls so that legislation in the areas for which itm8 is responsible is complied with to a sufficient extent. itm8 is not responsible for the applications running on the hosted equipment. Therefore, this statement does not include ensuring that sufficient controls have been established in the user applications and that the applications comply with the Danish Accounting Act, the Danish Personal Data Act and other relevant legislation.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

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

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

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

4.2 Test actions

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

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

4.3 Control objectives, control activity, tests and test results

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8'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 shall 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.* itm8 | Cloud & Infrastructure has established and documented an information security policy approved by top management and distributed to all employees. Additionally, several topic-specific policies have been developed to support the information security policy and are communicated to all relevant employees. These policies are reviewed at least annually or whenever significant changes occur.	We inquired Management regarding 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 and is reviewed annually.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.2	**Information security roles and responsibilities** *Information security roles and responsibilities shall be defined and allocated according to the organisation's needs.* itm8 | Cloud & Infrastructure has established clearly defined roles and responsibilities that are aligned with the requirements of its information security management system (ISMS). These roles are allocated based on the organisation's needs to ensure effective management and oversight of information security across the business.	We inquired Management regarding the procedures/control activities performed. We inspected that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No exceptions noted.
5.3	**Segregation of duties** *Conflicting duties and conflicting areas of responsibility shall be segregated.* itm8 | Cloud & Infrastructure has established policies for the segregation of duties, ensuring that conflicting responsibilities are properly separated. These policies are reviewed at least annually or whenever significant changes occur, ensuring alignment with the information security policy and maintaining the necessary level of segregation to safeguard information security.	We inquired Management regarding the procedures/control activities performed. By inspection of random samples, we investigated that the critical operating functions at itm8 have been appropriately segregated and that primary and secondary operating data have been segregated.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8’s control activity	Tests performed by PwC	Result of PwC’s tests
5.4	**Management responsibilities** ensure all personnel are aware of and fulfil their information security responsibilities *Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.* itm8 | Cloud & Infrastructure requires its management team to actively support and familiarise themselves with applicable information security initiatives. Management is also responsible for educating their employees on these initiatives to ensure compliance with the organisation's information security policies and procedures.	We inquired Management regarding the procedures/control activities performed. We inspected that Management is familiar with information security initiatives.	No exceptions noted.
5.5	**Contact with authorities** the organization and relevant legal, regulatory and supervisory authorities *The organisation shall establish and maintain contact with relevant authorities.* itm8 | Cloud & Infrastructure has established communication procedures for notifying relevant authorities in the event of a security incident.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has a communications procedure for how to communicate with relevant authorities in the case of a security incident.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.7	**Threat intelligence** *Information relating to information security threats shall be collected and analysed to produce threat intelligence.* itm8 | Cloud & Infrastructure collects threat intelligence from various sources, including vulnerability reports, selected news outlets, suppliers, authorities, and special interest groups, to support risk-based decision-making.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 collects and analyses information of information security threats.	No exceptions noted.
5.9	**Inventory of information and other associated assets** *An inventory of information and other associated assets, including owners, shall be developed and maintained.* itm8 | Cloud & Infrastructure has implemented and maintains various configuration management databases (CMDBs) tailored to the nature of the assets in scope. This includes inventories of endpoints, servers, networking equipment and databases, all of which have designated owners and relevant information assigned.	We inquired Management regarding 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 that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.10	**Acceptable use of information and other associated assets** *Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.* itm8 | Cloud & Infrastructure has established and implemented rules regarding the acceptable use of its assets, which are documented in the Policy for Acceptable Use.	We inquired Management regarding the procedures/control activities performed. We inspected that adequate controls are in place to ensure rules on acceptable use and procedures for handling information in itm8.	No exceptions noted.
5.12	**Classification of information** *Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability, and relevant interested party requirements.* itm8 | Cloud & Infrastructure has established a data classification scheme that outlines how different types of data must be classified and handled according to their classification.	We inquired Management regarding the procedures/control activities performed. By inspection, we verified that information is classified and that a Data Classification Scheme has been implemented.	No exceptions noted.
5.14	**Information transfer** *Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.* itm8 | Cloud & Infrastructure has established policies and procedures for information transfer, ensuring that information is transmitted through secure and reliable communication channels.	We inquired Management regarding the procedures/control activities performed. We inspected that an appropriate security architecture has been established in the network and that information transfer rules are in place.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.15	**Access control** *Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.* itm8 | Cloud & Infrastructure has implemented guidelines for access to its own and customer systems based on business and information security requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that guidelines on access controls have been established, reviewed and approved.	No exceptions noted.
5.18	**Access rights** *Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy and rules for access control.* itm8 | Cloud & Infrastructure regularly reviews employees' privileged technical rights in both internal and customer-facing systems to ensure they are ap-propriate for their work-related needs. Non-technical privileged employees are granted necessary rights for using internal systems, which are adjusted during employment changes, transfers, and terminations. When an employee leaves itm8, all access rights are revoked, and adjustments are made for any changes in job functions.	We inquired Management regarding the procedures/control activities performed. By inspection, we investigated that terminated users are removed in the operating environment in a timely manner after termination. Furthermore, we inspected that user access rights are reassessed once every six months.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.19	**Information security in supplier relationships** *Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of a supplier's products or services.* itm8 | Cloud & Infrastructure has established procedures for managing security risks related to supplier products and services, which include annual risk assessments and audits to ensure that suppliers continue to meet the organisation's security requirements.	We inspected that a formal and documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From samples of signed contracts, we inspected that risk assessments are performed regularly on critical suppliers. Furthermore, we inspected that itm8 audits key suppliers on a periodic basis, based on agreed information security requirements.	No exceptions noted.
5.20	**Addressing information security within supplier agreements** *Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.* itm8 | Cloud & Infrastructure has established security requirements for suppliers, which are included in the contractual agreements and the general terms and conditions for suppliers collaborating with itm8.	We inspected that a formal and 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 that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.22	**Monitoring, review, and change management of supplier services** *The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.* itm8 | Cloud & Infrastructure has established procedures for managing security risks associated with supplier products and services, which include annual risk assessments and audits to ensure compliance with the organisation's security requirements. Additionally, any changes in supplier services that impact customer environments, services or infrastructure are managed through itm8's change management process.	We inspected that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From a sample of signed contracts, we inspected that information security requirements have been contractually agreed. From a sample of months, we inspected that itm8 audits key suppliers on a periodic basis, based on agreed information security requirements. We inspected that third-party declarations have been received and processed by itm8 for key suppliers.	No exceptions noted.
5.23	**Information security for use of cloud services** *Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.* itm8 | Cloud & Infrastructure has established a strategy for using cloud services that aligns with the organisation's information security requirements, encompassing acquisition, management and exit processes.	We inspected that a strategy for the use of cloud services has been established.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.24	**Information security incident management, planning and preparation** *The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.* itm8 | Cloud & Infrastructure has defined and implemented a plan for managing information security incidents, which includes processes for incident management and handling, as well as clearly defined roles and responsibilities related to incident response.	We inspected that a formal and documented incident management process has been implemented. We inspected that roles and responsibilities related to the incident management process has been communicated to employees.	No exceptions noted.
5.26	**Response to information security incidents**itm8 | Cloud & Infrastructure has established procedures for responding to information security incidents.	We inspected that a formal and documented incident management process has been implemented. We inspected that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.27	**Learning from information security incidents:** To reduce the likelihood or consequences of future incidents *Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.* itm8 | Cloud & Infrastructure has established procedures for learning from information security incidents, ensuring that incidents are continuously re-viewed for opportunities to enhance the organisation's security posture.	We inspected that a formal and documented incident management process has been implemented. We inspected that all incidents have been registered, that necessary actions have been performed, and that security incidents have been reviewed.	No exceptions noted.
5.29	**Information security during disruption** *The organisation shall plan how to maintain information security at an appropriate level during disruption.* itm8 | Cloud & Infrastructure has established business continuity plans to ensure that the organisation can maintain information security and operations at an appropriate level during disruptions.	We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually. We inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.30	**ICT readiness for business continuity** *ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.* itm8 | Cloud & Infrastructure conducts annual ICT readiness tests to ensure that business continuity plans effectively support intended outcomes and that the organisation adheres to these plans.	We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually. We inspected that ICT readiness tests are performed annually and approved by relevant personnel.	No exceptions noted.
5.31	**Legal, statutory, regulatory and contractual requirements** *Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and kept up to date.* itm8 | Cloud & Infrastructure has documented all relevant legal, statutory, regulatory and contractual requirements related to information security that the organisation must comply with. This list is continuously updated to ensure accuracy.	We have observed that a formal policy for complying with relevant legislation is maintained, reviewed and approved. We have observed that a forum has been established for identifying applicable legislation and contractual requirements.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.34	**Privacy and protection of PII** *The organisation shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.* itm8 | Cloud & Infrastructure has identified applicable requirements for the preservation of privacy and protection of PII and has established adequate controls and measures to ensure compliance with these requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has established requirements regarding the preservation of privacy and protection of PII.	No exceptions noted.
5.36	**Compliance with policies, rules and standards for information security** *Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.* itm8 | Cloud & Infrastructure ensures compliance with its information security policy, topic-specific policies, rules and standards, which are regularly reviewed. Management supports and addresses the upholding of this compliance.	We have observed that formal meetings have been scheduled to review the policies, rules, standards etc. From a sample of meetings, we observed that meetings regarding information security have been held.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.37	**Documented operating procedures** *Operating procedures for information processing facilities shall be documented and made available to personnel who need them.* itm8 | Cloud & Infrastructure has established and documented operating procedures to support and manage the operation of solutions and services provided by the organisation. This includes a platform for communication and ensuring availability of these procedures to employees with a work-related need.	We inquired Management regarding 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 furthermore inspected that the operating procedures are accessible to all relevant employees.	No exceptions noted.

Control objective 6:

People controls

Procedures and controls ensure that human resource security is implemented and effective prior, during and after employment

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.1	**Screening** *Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis, take 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.* itm8 | Cloud & Infrastructure conducts screening of potential candidates, including obtaining clean criminal records for all employees. Employees are required to continuously provide a clean criminal record during their employment, which itm8 obtains every three years.	We inquired Management regarding the procedures/control activities performed. We inspected that an HR process is in place to ensure that criminal records are presented before employment starts for both employees and external consultants and every third year of employment. From samples of new hires, we inspected that criminal records have been acquired before employment start.	No exceptions noted.
6.2	**Terms and conditions of employment** *The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security.* itm8 | Cloud & Infrastructure has established terms and conditions of employment as part of the employment agreement between an employee and itm8. These include expectations for compliance with applicable information security initiatives.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 runs introductory courses for new employees during which terms and conditions of employment are included.	No exceptions noted.

Control objective 6:

People controls

Procedures and controls ensure that human resource security is implemented and effective prior, during and after employment

Nr.	itm8'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 shall 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.* itm8 | Cloud & Infrastructure conducts various security awareness initiatives continuously based on an annual plan and emerging security threats. This includes simulations of phishing attempts and other breach scenarios to enhance employees' hands-on experience. Furthermore, all employees are required to familiarise themselves with applicable information security requirements and the information security policy.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 performs annual security awareness initiatives and performs information security campaigns regularly. By inspection, we verified, that employees have been introduced to the Information Security Policy.	No exceptions noted.
6.5	**Responsibilities after termination or change of employment** *Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.* itm8 | Cloud & Infrastructure communicates information security responsibilities that remain in effect after termination or change of employment. This includes notifying the terminated employee of their continued obligations to confidentiality and non-disclosure.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 obtains a written confirmation of continued obligation after employment from terminated employees.	No exceptions noted.

Control objective 6:

People controls

Procedures and controls ensure that human resource security is implemented and effective prior, during and after employment

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.6	**Confidentiality or non-disclosure agreements** *Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.* itm8 | Cloud & Infrastructure establishes confidentiality agreements with its employees as part of the initial contractual employment agreements. Additionally, some employees may be subject to further confidentiality or non-disclosure agreements during their employment if required by customers.	We inquired Management regarding the procedures/control activities performed. By inspection of random samples, we verified that a non-disclosure agreement is signed as part of new employments.	No exceptions noted.
6.7	**Remote working** *Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.* itm8 | Cloud & Infrastructure has established and implemented security measures for personnel working remotely to ensure that the level of information security is comparable to when employees are working from the office. This includes, among other measures, the establishment of VPN connections and ensuring that all sensitive work is conducted on virtual desktops.	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures have been implemented for personnel working remotely.	No exceptions noted.

Control objective 6:

People controls

Procedures and controls ensure that human resource security is implemented and effective prior, during and after employment

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.8	**Information security event reporting** *The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.* itm8 | Cloud & Infrastructure has established a mechanism for personnel to report observed or suspected information security events. The procedure for utilising this mechanism is communicated to and made available to all employees.	We inquired Management regarding the procedures/control activities performed. We inspected that the incident management process has been communicated and made available to employees.	No exceptions noted.

Control objective 7:

Physical controls

Procedures and controls ensure that physical security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.2	**Physical entry** *Secure areas shall be protected by appropriate entry controls and access points.* itm8 | Cloud & Infrastructure has established physical entry controls for secure areas, which include identification cards, visitor registration and constant supervision of approved and cleared employees.	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that itm8 has implemented appropriate entry controls to protect physical facilities.	No exceptions noted.
7.3	**Securing offices, rooms and facilities** *Physical security for offices, rooms and facilities shall be designed and implemented.* itm8 | Cloud & Infrastructure has implemented physical security in its offices, which includes entry points accessible through personal ID cards and PIN codes, segregated security zones and CCTV surveillance.	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that itm8 has implemented appropriated entry controls to protect offices, rooms and facilities.	No exceptions noted.
7.4	**Physical security monitoring** *Premises shall be continuously monitored for unauthorised physical access.* itm8 | Cloud & Infrastructure has established CCTV at the entrances of both offices and data centres, as well as other facilities processing sensitive information.	We inspected that CCTV is established at entrances to both offices, data centres and other facilities processing sensitive information.	No exceptions noted.
7.6	**Working in secure areas** *Security measures for working in secure areas shall be designed and implemented.* itm8 | Cloud & Infrastructure has established procedures and guidelines for working in secure areas to ensure that work performed does not endanger employees or information assets.	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures have been established to secure employees and information assets.	No exceptions noted.

Control objective 7:

Physical controls

Procedures and controls ensure that physical security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.7	**Clear desk and clear screen** *Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.* itm8 | Cloud & Infrastructure has established a clear desk and clear screen policy to ensure that sensitive information is not left unattended in the office and that screens and endpoints are locked whenever they are left unattended.	We inquired Management regarding the procedures/control activities performed. We inspected that a clear desk and clear screen policy has been implemented.	No exceptions noted.
7.8	**Equipment siting and protection** *Equipment shall be sited securely and protected.* itm8 | Cloud & Infrastructure has a policy to ensure the protection of critical equipment.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has established guidelines on the protection against fire, water and heat. We furthermore inspected that itm8 has obtained an audit report from a subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	No exceptions noted.
7.9	**Security of assets off-premises** *Off-site assets shall be protected.* itm8 | Cloud & Infrastructure has established and communicated rules for the protection and handling of assets taken off-premises.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has established guidelines ensuring that off-site removal of equipment, information or software is subject to authorisation being granted prior to removal.	No exceptions noted.

Control objective 7:

Physical controls

Procedures and controls ensure that physical security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.10	**Storage media** *Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.* itm8 | Cloud & Infrastructure has established and implemented policies and procedures for handling storage media throughout their life cycle.	We inquired Management regarding the procedures/control activities performed. By inspection, we verified that itm8 has implemented formalised procedures for handling storage media throughout their life cycle.	No exceptions noted.
7.11	**Supporting utilities** *Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.* itm8 | Cloud & Infrastructure ensures that all equipment is maintained according to the manufacturer's specifications. Furthermore, itm8 ensures that its partners do the same.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has established a fully redundant infrastructure with individual backup.	No exceptions noted.
7.13	**Equipment maintenance** *Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.* itm8 | Cloud & Infrastructure ensures that equipment is maintained according to the manufacturer's specifications.	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures are implemented to ensure maintenance of equipment.	No exceptions noted.

Control objective 7:

Physical controls

Procedures and controls ensure that physical security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.14	**Secure disposal or re-use of equipment:** *Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.* itm8 | Cloud & Infrastructure has implemented guidelines for the disposal or re-use of equipment, ensuring that storage media is securely destroyed through certified vendors.	We inspected that itm8 has implemented procedures on secure disposal or re-use of equipment. We inspected that disposal and re-use of equipment is handled through a certified vendor.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.1	**User end point devices** *Information stored on, processed by or accessible via user end point devices shall be protected.* itm8 | Cloud & Infrastructure has implemented security policies for user end points, including remote wiping capabilities, malware protection, and other safeguards to ensure adequate protection.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has implemented a user end point device policy.	No exceptions noted.
8.2	**Privileged access rights** *The allocation and use of privileged access rights shall be restricted and managed.* itm8 | Cloud & Infrastructure has a policy for allocating and restricting privileged access. Users with privileged access have dedicated accounts for this purpose, and the privileged user access list is audited quarterly.	We inquired Management regarding the procedures/control activities performed. We inspected that itm8 has established formalised procedures for privileged user administration. We inspected that privileged access rights granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior. Furthermore, we inspected that privileged user access rights are reviewed quarterly.	No exceptions noted.
8.3	**Information access restriction**. *Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.* itm8 | Cloud & Infrastructure restricts access to systems and applications, ensuring only employees with a work-related need have the necessary permissions.	We inquired Management regarding the procedures/control activities performed. We inspected that a policy of limiting access to systems and applications to employees who have a work-related need has been implemented.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.5	**Secure authentication** *Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.* itm8 | Cloud & Infrastructure has implemented secure authentication technologies for sensitive information, including multi-factor authentication (MFA).	We inspected that a formal access control policy defining allowed technical solutions for authentication is maintained. We inspected that the access control policy has been reviewed and approved. We inspected that applications and systems in scope enforce secure log-on procedures.	No exceptions noted.
8.6	**Capacity management** *The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.* itm8 | Cloud & Infrastructure has procedures for monthly reporting on operations, including production environment capacity. Automatic monitoring of the operating environment and relevant system parameters ensures that future capacity requirements are met.	We inquired Management regarding the procedures/control activities performed. We inspected that reports on production environment operations at itm8 are sent to customers each month. We furthermore inspected that the capacity of production systems at itm8 is monitored to ensure that future capacity requirements are met.	No exceptions noted.
8.7	**Protection against malware** *Protection against malware shall be implemented and supported by appropriate user awareness.* itm8 | Cloud & Infrastructure has implemented procedures to ensure antivirus software is operational on all applicable systems, with continuous monitoring in place. User awareness is supported through itm8's security awareness platform, providing employees with knowledge on malware defence.	We inquired regarding the procedures/control activities performed. By inspection of random samples, we verified that antivirus software has been installed on all applicable systems and that antivirus software is monitored. Furthermore, we inspected that user awareness initiatives about antivirus software and malware defence have been established for employees.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.8	**Management of technical vulnerabilities** *Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.* itm8 | Cloud & Infrastructure has a procedure for continuously assessing reported vulnerabilities, evaluating their criticality using multiple sources and taking appropriate action in relation to the services provided.	We inquired regarding the procedures/control activities performed. By inspection using random samples, we noted that technical vulnerabilities of information systems are obtained in a timely fashion and evaluated, and appropriate measures taken to address the associated risk. Furthermore, we inspected that critical vulnerabilities are communicated to all relevant stakeholders.	No exceptions noted.
8.9	**Configuration management** *The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.* itm8 | Cloud & Infrastructure has established processes and procedures for configuration management to ensure that changes to configuration items are handled and documented properly.	We inquired Management regarding the procedures/control activities performed. We inspected that resources are monitored and adjusted in line with the current procedures for configuration management.	No exceptions noted.
8.10	**Information deletion** *Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.* itm8 | Cloud & Infrastructure has established procedures for information deletion to ensure that no data is stored longer than required by regulatory or business requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that information is deleted in line with itm8's procedures.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.13	**Information backup** *Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.* itm8 | Cloud & Infrastructure performs backups in accordance with itm8's best practices or customer business requirements. The backup jobs are monitored to ensure continuous operation, and an annual recovery test is initiated by itm8.	We inquired Management regarding the procedures/control activities performed. We inspected that requirements regarding backup have been established in the contract with sub-contractors that provide services where backup is relevant. We inspected that a full restore test of IT environments has been performed.	No exceptions noted.
8.14	**Redundancy of information processing facilities** *Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.* itm8 | Cloud & Infrastructure has redundancy in its own information processing facilities and can provide additional redundancy to meet customer requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that redundancy has been implemented on itm8's information processing facilities and on customer environments according to signed customer contracts.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8'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 shall be produced, stored, protected and analysed.* itm8 | Cloud & Infrastructure performs security information and event management (SIEM) on its own systems and for customers as required. Logs are recorded for various systems at different security levels, with full segregation of duties in the SIEM system. Employees who can delete log data do not have access to customer or itm8 systems. All access to customer systems is logged in the asset management system, securely stored and set up to audit any attempts to alter the information.	We inquired Management regarding the procedures/control activities performed. We inspected that logging of user activities, exceptions, faults and information security events has been configured. We inspected that all user access activity to customer data is logged. Furthermore, we inspected that sufficient segregation of duties have been implemented to log systems.	No exceptions noted.
8.16	**Monitoring activities** *Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.* itm8 | Cloud & Infrastructure has implemented a monitoring system that ensures customer systems are operational, with alerts for any anomalous behaviour. The system is monitored 24/7.	We inquired Management regarding the procedures/control activities performed. We inspected that a monitoring system has been implemented and that the system is monitored 24/7.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8'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 shall be synchronised to approved time sources.* itm8 | Cloud & Infrastructure has synchronised all relevant information processing systems to a single reference time source.	We inquired regarding the procedures/control activities performed. We inspected that itm8 has established a reference time source for clock synchronisation of all relevant information processing systems.	No exceptions noted.
8.19	**Installation of software on operational system** *Procedures and measures shall be in place to securely manage software installation on operational systems.* itm8 | Cloud & Infrastructure has defined a set of standard implementation descriptions for software installations. These standards are enforced on customer systems to ensure secure management.	We inquired Management regarding the procedures/control activities performed. We inspected that software installation on operational systems are managed appropriately and according to current procedures.	We have noted that two Domain Controller servers have not been patched aligned with approved procerus. We have received evidence after our test that these servers have been patched properly. No further exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.20	**Networks security** *Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.* itm8 | Cloud & Infrastructure has implemented several policies to ensure secure communication and minimise data tampering. Access to network devices is restricted to employees with a work-related need. Communication between itm8 and customer sites uses valid and proven secure technologies.	We inquired regarding the procedures/control activities performed. By inspection, we investigated whether – in accordance with guidelines – an appropriate security architecture has been established in the network, including whether: • the network is segregated into secure zones and whether customer environments are separated from itm8's own environment. • remote access is granted through two-factor authentication. • changes to the network environment included in our sample have been made in a controlled manner in accordance with the change management rules.	No exceptions noted.
8.22	**Segregation of networks** *Groups of information services, users and information systems shall be segregated in the organisation's networks.* itm8 | Cloud & Infrastructure segregates customer networks into one or more networks based on the need for segregation, ensuring that customers cannot access other customer networks.	We inquired Management regarding the procedures/control activities performed. We inspected the technical security architecture and, by inspection of random samples, we investigated whether – in accordance with guidelines – an appropriate security level has been established, including whether: • secure zones and customer environments are separated from itm8's own environment • access to the network is segregated into relevant user groups based on users' work-related need.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.23	**Web filtering** *Access to external websites shall be managed to reduce exposure to malicious content.* itm8 | Cloud & Infrastructure has implemented web filtering measures to protect against and reduce exposure to malicious content.	We inquired Management regarding the procedures/control activities performed. We inspected that web filtering measures have been implemented.	No exceptions noted.
8.24	**Use of cryptography** *Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.* itm8 | Cloud & Infrastructure has established policies on the use of cryptography, including rules for usage, selection of cryptographic techniques, implementation, maintenance and disposal.	We inquired Management regarding the procedures/control activities performed. We inspected that appropriate use of cryptography and cryptographic key management have been established.	No exceptions noted.
8.32	**Change management** *Changes to information processing facilities and information systems shall be subject to change management procedures.* itm8 | Cloud & Infrastructure has established and implemented a change management process to ensure that all changes to information systems in production environments are properly managed, avoiding unnecessary conflicts and ensuring fallback plans are in place.	We inquired regarding the procedures/control activities performed. We inspected that itm8 has drawn up procedures for annual review and updating of: • Incident management • Problem management • Change management • Release and patch management • User administration.	No exceptions noted.

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

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

Frank Bech Jensen
Kunde
Serienummer: 4ecdf2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c
IP: 93.165.xxx.xxx
2025-02-03 20:06:04 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-03 20:19:00 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 83.136.xxx.xxx
2025-02-03 20:20:08 UTC

Penneo dokumentnøgle: 1Y2OC-ZY0FZ-BFEN2-3YOJ8-QXNGJ-BAKV2

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

Dette dokument er forseglet med et kvalificeret elektronisk segl med brug af certifikat og tidsstempel fra en kvalificeret tillidstjenesteudbyder.

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