



itm8 A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2025 to 31 December 2025 in relation to services provided by itm8 | Managed Services to customers

February 2026



Contents

1. Management's assertion	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 assertion

The accompanying description has been prepared by itm8 A/S (itm8) for customers who have used services provided by itm8 | Managed 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 their financial statements.

Fuzion and InterXion are service organisations that provide housing services to itm8, and B4Restore and Keepit are service organisations that provide backup services to itm8. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of itm8 and excludes the control objectives and related controls of Fuzion, InterXion, B4Restore and Keepit. Our evaluation did not extend to controls of Fuzion, InterXion, B4Restore and Keepit.

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

itm8 confirms that:

- a) The accompanying description in section 3 fairly presents the services provided by itm8 | Managed Services that have processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how IT general controls in relation to the services provided by itm8 | Managed 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 the services provided by itm8 | Managed 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 IT general controls
 - (ii) Includes relevant details of changes to IT general controls in relation to the services provided by itm8 | Managed Services during the period from 1 January 2025 to 31 December 2025
 - (iii) Does not omit or distort information relevant to the scope of IT general controls in relation to the services provided by itm8 | Managed 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 IT general controls in relation to the services provided by itm8 | Managed 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 2025 to 31 December 2025. The criteria used in making this statement were that:

- (i) The risks that threatened achievement of the control objectives stated in the description were identified
- (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved
- (iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.

Herning, 17. February 2026
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 2025 to 31 December 2025 in relation to services provided by itm8 | Managed Services to customers

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

Scope

We have been engaged to report on itm8's description in section 3 of IT general controls in relation to the services provided by itm8 | Managed Services which have processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Fuzion and InterXion are service organisations that provide housing services to itm8, and B4Restore and Keepit are service organisations that provide backup services to itm8. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of itm8 and excludes the control objectives and related controls of Fuzion, InterXion, B4Restore and Keepit. Our examination did not extend to controls of Fuzion, InterXion, B4Restore and Keepit.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of itm8's controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

itm8's responsibilities

itm8 is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives. The control objectives have been specified by itm8 and are stated in the description.

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of itm8's description and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

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

An assurance engagement to report on the description of a service organisation's system and the suitability of the design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the description and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by itm8 and described in section 1.

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

Inherent limitations

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 services provided by itm8 | Managed Services that the individual customer may consider important in its own particular circumstances. Also, because of their nature, controls at a service organisation or subservice organisation may not prevent or detect all errors or omissions in the services provided by itm8 | Managed Services. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria including the control objectives described in itm8's assertion in section 1:

- a) The description fairly presents how IT general controls in relation to the services provided by itm8 | Managed Services were designed and implemented throughout the period from 1 January 2025 to 31 December 2025
- b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2025 to 31 December 2025 and user entities applied the complementary customer controls referred to in section 3
- c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

Description of test of controls

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

Intended users and purpose

We were engaged to report by itm8 and, therefore, this report and the description of tests of controls and results thereof in section 4 are intended for the use of itm8.

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by itm8, at its discretion, to customers who have used the services provided by itm8 | Managed Services during some or all of the period of 1 January 2025 to 31 December 2025 and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

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

Aarhus, 17. February 2026

PricewaterhouseCoopers

Statsautoriseret Revisionspartnerselskab



CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

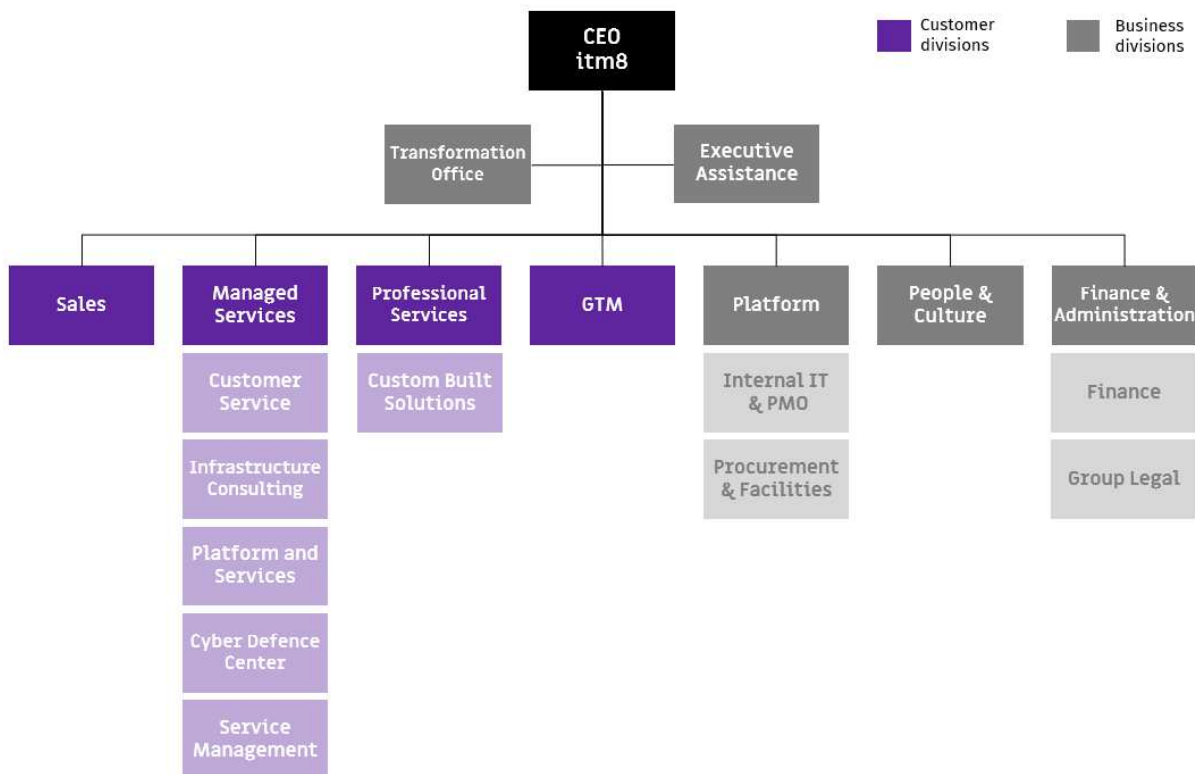
Iraj Bastar
director

3. Service organisation's system description

3.1. Description of the service organisation

itm8 A/S has undergone a significant development and has become a structured organisation that provides managed IT services and professional services. itm8 A/S Denmark is established on the basis of 12 independent IT companies, all of which are owned by the itm8 Group. All 12 companies have now been legally and organisationally merged into itm8 A/S, which in addition to the Danish locations also includes itm8's global delivery locations in the Czech Republic and the Philippines. As a natural part of the merger, a major transition is now taking place in consolidating and unifying services, processes and systems.

All companies have been merged into itm8 A/S's customer-oriented departments that drive service deliveries, while business divisions ensure necessary administrative and operational support. This structure enables itm8 to provide integrated and reliable services that meet high requirements in information security, quality and compliance to a wide range of customers.



Scope of itm8 | Managed Services ISAE 3402 independent assurance report

This independent assurance report focuses on itm8 Managed Services, which is the central part of the report's scope. The division offers cloud solutions and IT infrastructure services that meet itm8's standards for secure and quality-oriented service delivery. A key part of these deliverables are elements from itm8 Cybersecurity, including the Cyber Defense Center, which plays a critical role with 24/7 monitoring, SIEM log management, and incident management, all of which are critical to infrastructure security.

In addition, components from itm8 Professional Services, Custom Built Solutions, which develops tailor-made solutions such as SEPO Send Safely and the Dental Record system TK2, are involved. These specialised solutions support itm8's commitment to providing secure and customised services that meet the unique needs of its customers.

Customer divisions

The customer-oriented divisions constitute itm8's primary service areas, with each division dedicated to specific areas of expertise:

- **itm8 | Managed Services**

With a focus on cloud solutions and IT infrastructure, this division helps customers implement robust hosting and operations strategies. The division translates customers' business strategies into scalable cloud and infrastructure solutions through platform evaluations, security policy design, migrations, modernization and 24/7 support.

Managed Services provides services to customers within service desk, operations, application operations and consulting services. Managed Services also includes the Cyber Defense Center, which is a division that offers comprehensive security services such as ongoing SIEM log management, vulnerability assessments, and real-time incident management via a 24X7 Security Operation Center.

- **itm8 | Professional Services | Custom Built Solutions**

This division drives digital innovation for customers, offering ERP integration, SharePoint and Microsoft solutions, as well as unique products developed by Team Products, such as the Send Secure platform and the Dental Record system (TK2), to optimise business processes.

Business divisions

In support of these core areas, itm8's business divisions such as HR, Finance, Marketing, Legal, Internal IT and Compliance & Security provide a solid base for effective service delivery. These divisions are critical to itm8's operational integrity and ensure that all customer-facing activities are compliant with itm8's standards and regulatory requirements.

Together, these divisions create a robust structure that enables itm8 to provide specialised and high-quality services that support customers' strategic goals.

3.2. Information security management system

The information security management system (ISMS) at itm8 is designed to meet the requirements of ISO 27001:2022 and integrate information security into our organisational processes and culture.

Organisational context:

Our ISMS is aligned with itm8's context and takes into account our strategic goals, external and internal challenges and stakeholder needs and expectations. Through stakeholder analyses, we ensure that our information security measures are in line with the expectations of relevant parties and adapted to a changing risk landscape.

Management:

Management commitment is a cornerstone of our ISMS. The top management has defined and approved an appropriate and effective information security policy that establishes the organisation's information security goals and ensures coherence with the overall business goals. Management works actively to promote a safety culture, allocate sufficient resources and clearly communicate and anchor roles and responsibilities throughout the organisation.

Planning:

The planning of our ISMS is based on a structured risk management process and methodology, supported by a dedicated system. We carry out regular risk assessments to identify, evaluate and mitigate risks and ensure that they are managed within acceptable levels. Information security objectives are set, reviewed periodically and integrated into the company's overall strategic planning to ensure a proactive approach to risk management.

Support:

Our ISMS is supported by a document management system (DMS) that securely stores all official documentation and meets strict quality requirements. In addition, we maintain a comprehensive security awareness programme, offering ongoing training and testing to ensure that all employees understand their role in maintaining and improving information security. The programme focuses on competence development and increased awareness across the organisation.

Operations:

We implement and manage our processes based on the ITIL framework, ensuring that all operations are in line with best practices and our defined information security goals. Our operational approach integrates security into day-to-day business activities, making security a natural part of the organisation. The DMS serves as a central platform for all processes, procedures and policies, ensuring that operational activities are compliant with the ISMS.

Performance evaluation:

To 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, combined with management reviews and other performance metrics, provide critical insights that help us maintain compliance with ISO 27001, new and changing business needs and continuously address the current threat landscape. The results are used for continuous improvement and ensure that our ISMS remains efficient and up to date.

Improvement:

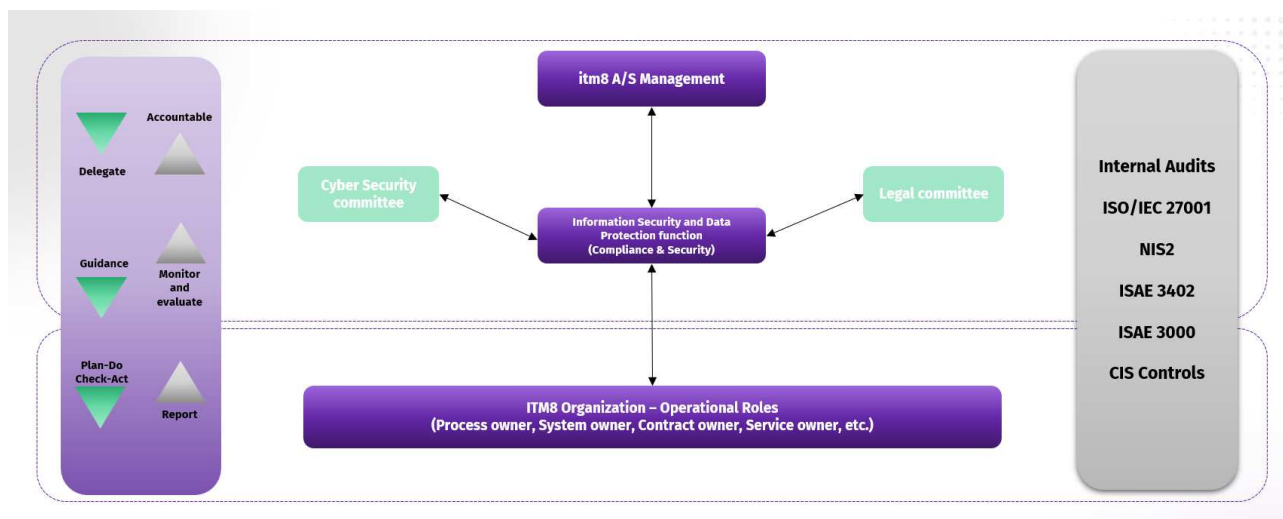
Continuous improvement is integrated into our ISMS through quarterly Continuous Improvement (CIM) meetings within the Compliance & Security team. These meetings, where official minutes are kept, provide a platform to discuss all aspects of information security at itm8. Insights from the meetings, internal audits and performance evaluations are used to drive improvements in our ISMS. We are committed to a cycle of continuous evolution to ensure that our ISMS remains dynamic and effective in addressing emerging threats and in line with industry's best practices.

3.3. Information security management

Information security management at itm8 is designed to ensure that security practices are integrated throughout the organisation in accordance with ISO/IEC 27001:2022. Our approach starts with an information security policy, approved by senior management, that outlines our information 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 & Security team. Relevant policies are communicated to the affected stakeholders.

We have clearly defined roles in information security, including functions such as information security manager, system owner and process owner, to ensure that responsibilities are clearly assigned and understood. Feature separation is implemented in critical areas such as backup, finance, change management and development to reduce risks associated with unauthorised access or failure.

Our information security management structure places overall responsibility with senior management who delegates tasks to the Compliance & Security team. This team collaborates with the Cybersecurity and Legal Commissions to handle technical and legal security aspects.



itm8 security management structure

Management plays a critical role in supporting our information security framework, ensuring compliance with applicable requirements, and actively participating in the governance of our ISMS. We maintain an up-to-date list of all relevant authorities and legislation with associated responsible owners to ensure compliance and facilitate communication with regulators. Our participation in various interest groups, such as security forums and IT networking groups, keeps us up to date on industry trends and best practices.

Information security is also integrated into our project management practices through a risk-based approach to managing projects that requires project managers to carry out an initial risk assessment at the start of a project. This ensures that security considerations are addressed early in the project lifecycle, further embedding information security in our organisational processes and culture.

3.4. Asset management

itm8 manages its information and associated assets in accordance with ISO/IEC 27001:2022 standards. We maintain asset inventories through various databases, including a primary CMDB for CIs and customer-facing solutions, as well as InTune MDM for endpoint management. Clear policies and safety guides outline acceptable use and ensure that all employees understand how to handle assets responsibly.

Asset return procedures are integrated into our HR processes to ensure safe return when employees leave the company or change roles. We have established guidelines for securing assets outside the company as well as for handling storage media on both endpoint devices and customer-facing platforms such as servers.

There are procedures for the safe disposal and recycling of equipment, which include both internal and customer-facing assets, ensuring that all data is properly erased. The user's endpoint devices are centrally managed and associated with the domain, which allows us to enforce security configurations and maintain control over those assets.

3.5. Information protection

At itm8, we ensure effective information protection in accordance with ISO/IEC 27001:2022 controls. We have established a classification scheme described in our *Principles & Rules for Information Protection*, which guides the classification and labelling of information based on its sensitivity. This ensures that all information is handled correctly in relation to its classification.

To protect data in transit, we have developed specific rules and policies, including security guides, that describe secure methods of information exchange. Protection of records is handled through standard system design and established procedures, with a particular focus on privacy protection and compliance with the EU's GDPR for personal data (PII).

We have clear procedures for deleting information to ensure that data is removed securely when it is no longer needed. Data masking is applied using test data from production environments to maintain privacy and security, even during test scenarios.

To prevent data leaks, we have implemented monitoring activities designed to detect and remediate unauthorised data exposure. Test information is protected in accordance with our established standards and relevant agreements, ensuring that it is treated with the same care as live data.

3.6. HR security

Human resources security at itm8 is managed in accordance with ISO/IEC 27001:2022 to ensure that all staff are adequately assessed, trained and held accountable for their roles in information security. We conduct background checks on employees upon employment, which includes obtaining a clean criminal record for critical staff. This check is repeated every three years of employment to maintain a high level of reliability.

Our terms of employment contain specific clauses related to information security, ensuring that all employees understand their obligations. We have a security awareness programme that includes 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 that is applied when necessary to enforce our security policies. Following termination or changes in employment, we handle access rights carefully and they are revoked or adjusted as necessary to maintain security.

Non-disclosure and non-disclosure agreements are integral parts of our employment contracts, with additional agreements for certain roles depending on the client's requirements. For remote work, we have established specific rules and guidelines outlined in our safety guides to ensure that employees maintain safety standards when working outside the office.

3.7. Security awareness

itm8 works with structured programmes for employees around training and testing in security. The programmes start at employment as an onboarding process and then continue continuously with regularly planned training modules and testing of the organisation's resistance to phishing email.

Training consists of a combination of standard safety training and customised training which is targeted at itm8's own guidelines and requirements.

3.8. Physical security

ITM8 maintains robust physical security measures in accordance with ISO/IEC 27001:2022 to protect our assets and facilities. Physical security perimeters are established in both office and data centre locations where areas that require protection and the necessary security measures are defined. Physical access to these locations is controlled through the use of ID cards, PIN codes and alarm systems and CCTV surveillance at central access points.

Offices, spaces and facilities are secured based on their sensitivity, with defined security zones that have tailored measures to protect against unauthorised access. We implement protection against physical and environmental threats and adapt security controls according to the sensitivity of the information in a particular area.

Guidelines and procedures for working in safe areas are in place to maintain a high level of safety in these environments. A policy on tidy tables and screens is enforced, and expectations are communicated through our safety guides to ensure that sensitive information is not left exposed.

Equipment is positioned and protected based on its sensitivity and purpose, with secure locations ensuring the safety and integrity of the hardware. Support functions are adapted to the needs of each location; for example, data centres and other critical locations are equipped with emergency generators and UPS systems to maintain operations during power outages.

We also ensure that all equipment is professionally maintained according to the manufacturer's recommendations, so that it operates efficiently and remains safe throughout its life cycle. Cable installations are handled securely to prevent tampering and unauthorised access, and all maintenance activities are carried out to maintain the highest standards of operational safety.

3.9. System and network security

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

To protect against malware, we implement and monitor protection measures on our internal infrastructure and extend these services to customer environments as agreed. Use of privileged utility applications is limited 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 that are tailored to protect both manufacturing and office networks. Network services are set up securely, in accordance with best practices and customer agreements, and ensure that the services meet contractual and security requirements.

We maintain strict network segregation, where manufacturing and office networks are kept separate, and customers' networks are 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 harmful web pages, and breaches of these security measures 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 in CAB meetings to ensure that potential impacts are fully assessed and mitigated, maintaining the security and stability of our systems and networks.

3.10. Application security

ITM8 handles application safety in accordance with ISO/IEC 27001:2022 controls. Access to source code is restricted to those employees who need it, ensuring that sensitive code is protected. We have implemented a secure development cycle that integrates security requirements adapted to the criticality of the applications.

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

For outsourced development, specific guidelines ensure that security standards are met. Development, test and production environments are kept separate to prevent interference and maintain system integrity.

3.11. Secure configuration

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

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

3.12. Identity and access management

At itm8, we adhere to ISO/IEC 27001:2022 controls to protect access to systems and information. We have implemented an access control policy and associated procedures to effectively regulate access.

Identity management is handled in collaboration between human resource management, user management and HR and covers the entire user identity lifecycle. Authentication practices are defined for both customer-facing and internal environments, ensuring that secure methods are in place.

Access rights are granted based on job requirements, and we limit privileged access to only necessary personnel. Specific rules govern the handling 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 it is critical to increase security.

3.13. Threat and vulnerability management

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

Our management of technical vulnerabilities is guided by a defined procedure, which includes ongoing vulnerability assessments and management in our own internal environment, with responsibilities assigned to technology owners to ensure timely identification and remediation of vulnerabilities.

3.14. Continuity

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

Capacity management is handled 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 handled by an ISO/IEC 27001-certified third-party vendor. These backups are stored in geolocated facilities separate from the original production environment to ensure their availability, even during major disruptions.

3.15. Security in supplier relationships

At itm8, we handle supplier relationships with a strong focus on information security. Our agreements with suppliers often include security addenda where possible and relevant, and we actively monitor suppliers' operations for potential issues.

A formal vendor onboarding procedure ensures that vendors are categorised and evaluated before agreements are made. We continuously perform risk assessments for critical suppliers to manage potential risks effectively.

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

3.16. Compliance

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

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

We conduct ongoing independent reviews of our information security practices, including ISAE 3402 and ISAE 3000 audits for hosting services and data protection, as well as audits of customers and external audits in accordance with our ISO 27001 certification. We use the experiences, observations and feedback from audits as part of our improvement process and ensure that these are processed and addressed in the organisation.

We remain compliant with relevant information security policies, regulations and standards and continuously update our practices to ensure that we follow the relevant frameworks and that our measures reflect the applicable compliance requirements.

3.17. Handling of information security incidents

We handle information security incidents through a structured incident management process that includes procedures for major incidents and security incidents. These procedures outline roles, responsibilities and the steps needed to assess, respond to and learn from incidents.

We ensure thorough collection of evidence during incident management to support analysis and provide documentation for review. Information security incidents are reported to Top Management on an ongoing basis 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 monitors activities around the clock, while maintaining clock synchronisation to ensure accurate timestamps for alarms, providing a reliable overview of events and IT environment operations.

As part of the handling of information security incidents, lessons learned are used to ensure learning from the incident in order to create improvements that can reduce the risk of similar incidents occurring.

In conclusion, it is important to emphasise that the work with compliance and information security is an ongoing process where continuous improvement is at the centre. Itm8 commits to systematically evaluating and optimising existing procedures so that they always meet current requirements and best practices.

By actively incorporating experience from incident management, internal and external audits, as well as by strengthening the employees' competencies and implementing relevant key figures, a robust and future-proof level of information security is ensured. Going forward, itm8 will continue to invest in developing and anchoring a strong compliance and security culture that can meet current and future challenges.

3.18. Significant changes

There have been no significant changes to procedures and controls in the period from 1 January 2025 to 31 December 2025.

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

3.19. Complementary controls at the customers

Matters to be considered by the customers' auditors

Services provided

The above system description of controls is based on itm8's standard terms. The customers' deviations from itm8's standard terms are therefore not covered by this statement. The 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 operating effectiveness of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

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

4.2. Test actions

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

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.
Inquiries	Inquiry of appropriate personnel. Inquiries included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

4.3. Overview of 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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.1	<p>Policies for information security <i>Information security policies 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.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that a Management-approved and updated security policy is in place.</p> <p>We inspected that the information security policies are communicated to employees and relevant parties and are reviewed annually.</p>	No exceptions noted.
5.2	<p>Information security roles and responsibilities <i>Information security roles and responsibilities shall be defined and allocated according to the organisation needs.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that the organisational areas of responsibility have been defined and allocated to relevant personnel.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.3	<p>Segregation of duties <i>Conflicting duties and conflicting areas of responsibility shall be segregated.</i></p> <p>itm8 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.</p>	<p>We inquired Management regarding the procedures/control activities performed.</p> <p>We inspected that the critical operating functions at itm8 have been appropriately segregated and that primary and secondary operating data have been segregated.</p>	No exceptions noted.
5.4	<p>Management responsibilities <i>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.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that Management is familiar with information security initiatives.</p>	No exceptions noted.
5.5	<p>Contact with authorities <i>The organisation shall establish and maintain contact with relevant authorities.</i></p> <p>itm8 has established communication procedures for notifying relevant authorities in the event of a security incident.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 has a communications procedure for how to communicate with relevant authorities in the case of a security incident.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.6	<p>Contact with special interest groups <i>The organisation shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.</i></p> <p>itm8 participates in various specialist groups for various aspects of information security which is utilised to improve the basis of information security in itm8 and gather knowledge on vulnerabilities and relevant information security initiatives.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that the organisational areas of responsibility have been defined and allocated to relevant personnel.</p>	No exceptions noted.
5.7	<p>Threat intelligence <i>Information relating to information security threats shall be collected and analysed to produce threat intelligence.</i></p> <p>itm8 collects threat intelligence from various sources, including vulnerability reports, selected news outlets, suppliers, authorities and special interest groups, to support risk-based decision-making.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 collects and analyses information of information security threats.</p>	No exceptions noted.
5.8	<p>Information security in project management <i>Information security shall be integrated into project management.</i></p> <p>itm8 has established procedures for risk assessment as part of our project management process to address information security risks before and during project implementation.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a policy for information security in project management is in place.</p> <p>Using samples, we furthermore inspected that information security is integrated into project management and that itm8 has conducted risk assessments as an integrated part of the project management process.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.9	<p>Inventory of information and other associated assets</p> <p><i>An inventory of information and other associated assets, including owners, shall be developed and maintained.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.</p>	No exceptions noted.
5.10	<p>Acceptable use of information and other associated assets</p> <p><i>Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.</i></p> <p>itm8 has established and implemented rules regarding the acceptable use of its assets, which are documented in the Policy for Acceptable Use.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that adequate controls are in place to ensure rules on acceptable use and procedures for handling information in itm8.</p>	No exceptions noted.
5.11	<p>Return of assets</p> <p><i>Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.</i></p> <p>itm8 has established procedures for the safe return of assets upon termination or change of employment to ensure sensitive organisational information does not leave the control of the itm8.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that a procedure is in place to ensure that assets are returned upon termination.</p> <p>By inspection of a sample of terminated employees, we observed that there is documentation of confirmation that all assets have been returned upon termination.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.12	<p>Classification of information <i>Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements.</i> itm8 has established a data classification scheme that outlines how different types of data must be classified and handled according to their classification.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected that information is classified and that a data classification scheme has been implemented.</p>	No exceptions noted.
5.13	<p>Labelling of information <i>An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.</i> itm8 has a policy for labelling of information according to our data classification scheme.</p>	<p>We made inquiries of Management about the procedures/control activities performed. We observed that a classification scheme is maintained and has been made available for employees. We observed that the classification scheme has been reviewed and approved.</p>	No exceptions noted.
5.14	<p>Information transfer <i>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.</i> itm8 has established policies and procedures for information transfer, ensuring that information is transmitted through secure and reliable communication channels.</p>	<p>We inquired of 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.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.15	<p>Access control <i>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.</i> itm8 has implemented guidelines for access to its own and customer systems based on business and information security requirements.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected that guidelines on access controls have been established, reviewed and approved.</p>	No exceptions noted.
5.16	<p>Identity management <i>The full life cycle of identities shall be managed.</i> itm8 manages identities in its full life cycle from registration to de-registration ensuring that identities have the appropriate and required access for their function and nothing more.</p>	<p>We made inquiries of Management about the procedures/control activities performed. We inspected that procedures include the full lifecycle of an identity.</p>	No exceptions noted.
5.17	<p>Authentication information <i>Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.</i> itm8 manages and performs allocation of authentication information through a controlled management process that likewise ensure authentication information are generated at random and comply with the organisation's policy for complexity of authentication information.</p>	<p>We made inquiries of Management about the procedures/control activities performed. We inspected that itm8 has established formalised procedures for authentication information covering usernames, passwords and certificates.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.18	<p>Access rights <i>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.</i></p> <p>itm8 regularly reviews employees' privileged technical rights in both internal and customer-facing systems to ensure they are appropriate 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that terminated users are removed in the operating environment in a timely manner after termination.</p> <p>Furthermore, we inspected that user access rights are reassessed every six months.</p>	<p>During our audit, we found that the executed user-management controls were not documented sufficiently in accordance with the applicable procedures. Furthermore, documentation was not available for all periodic reviews of privileged user access for two management domains.</p> <p>We have been informed that the controls were performed, but they were not documented. In our samples, we did not identify any deviations.</p> <p>No further deviations noted.</p>
5.19	<p>Information security in supplier relationships <i>Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.</i></p> <p>itm8 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.</p>	<p>We inspected that a formal and documented procedure is in place to ensure that new or renegotiated application or service supplier contracts are validated against a list of defined information security requirements.</p> <p>We inspected that risk assessments are performed regularly on critical suppliers.</p> <p>Furthermore, we inspected that itm8 audits key suppliers on a periodic basis, based on agreed information security requirements.</p>	<p>No exceptions noted.</p>

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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.20	<p>Addressing information security within supplier agreements</p> <p><i>Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.</i></p> <p>itm8 has established security requirements for suppliers, which are included in the contractual agreements and the general Terms and Conditions for suppliers collaborating with itm8.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a formal and documented procedure is in place to ensure that new or renegotiated application or service supplier contracts are validated against a list of defined information security requirements.</p>	No exceptions noted.
5.21	<p>Managing information security in the information and communication technology (ICT) supply chain</p> <p><i>Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.</i></p> <p>itm8 has established procedures for managing security risks associated with the use of a supplier's products and services which include a yearly risk assessment and audit of suppliers to ensure supplier continue to live up to the security requirements itm8 expects.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.22	<p>Monitoring, review and change management of supplier services</p> <p><i>The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.</i></p> <p>itm8 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.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>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.</p> <p>From a sample of signed contracts, we inspected that information security requirements have been contractually agreed.</p> <p>From a sample of months, we inspected that itm8 audits key suppliers on a periodic basis, based on agreed information security requirements.</p> <p>We inspected that third-party declarations have been received and processed by itm8 for key suppliers.</p>	No exceptions noted.
5.23	<p>Information security for use of cloud services</p> <p><i>Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.</i></p> <p>itm8 has established a strategy for using cloud services that aligns with the organisation's information security requirements, encompassing acquisition, management and exit processes.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a strategy for the use of cloud services has been established.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.24	<p>Information security incident management planning and preparation</p> <p><i>The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.</i></p> <p>itm8 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.</p>	<p>We inspected that a formal and documented incident management process has been implemented.</p> <p>We inspected that roles and responsibilities related to the incident management process has been communicated to employees.</p>	No exceptions noted.
5.25	<p>Assessment and decision on information security events</p> <p><i>The organisation shall assess information security events and decide if they are to be categorised as information security incidents.</i></p> <p>itm8 has established procedures for assessing information security events to determine if such events should be classified as security incidents.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that a formal and documented incident management process related to information security events and breaches has been implemented.</p> <p>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 and reported through the Compliance & Security.</p>	No exceptions noted.
5.26	<p>Response to information security incidents</p> <p><i>Information security incidents shall be responded to in accordance with the documented procedures.</i></p> <p>itm8 has established procedures for responding to information security incidents.</p>	<p>We inspected that a formal and documented incident management process has been implemented.</p> <p>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.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.27	<p>Learning from information security incidents <i>Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.</i></p> <p>itm8 has established procedures for learning from information security incidents, ensuring that incidents are continuously reviewed for opportunities to enhance the organisation's security posture.</p>	<p>We inspected that a formal and documented incident management process has been implemented.</p> <p>We inspected that all incidents have been registered, that necessary actions have been performed, and that security incidents have been reviewed.</p>	No exceptions noted.
5.28	<p>Collection of evidence <i>The organisation shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.</i></p> <p>itm8 has established mechanisms and procedures for the collection of evidence related to information security events, to ensure that learning opportunities are gained on basis of proper evidence.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that a formal process for assessment and analysis of information security incidents is maintained.</p> <p>Based on a sample of two months, we observed that Compliance & Security reviews and analyses incidents categorised as information security incidents.</p>	No exceptions noted.
5.29	<p>Information security during disruption <i>The organisation shall plan how to maintain information security at an appropriate level during disruption.</i></p> <p>itm8 has established business continuity plans to ensure that the organisation can maintain information security and operations at an appropriate level during disruptions.</p>	<p>We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually.</p> <p>We inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.30	<p>ICT readiness for business continuity <i>ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.</i> itm8 conducts annual ICT readiness tests to ensure that business continuity plans effectively support intended outcomes and that the organisation adheres to these plans.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually.</p> <p>We inspected that ICT readiness tests are performed annually and approved by relevant personnel.</p>	No exceptions noted.
5.31	<p>Legal, statutory, regulatory and contractual requirements <i>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.</i> itm8 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.</p>	<p>We made inquiries of Management about the procedures and control activities performed.</p> <p>We observed that a formal policy for complying with relevant legislation is maintained, reviewed and approved.</p> <p>We inspected that the list of legal, statutory, regulatory, and contractual requirements is documented and that the list has been reviewed and approved by appropriate and competent personnel.</p>	No exceptions noted.
5.32	<p>Intellectual property rights <i>The organisation shall implement appropriate procedures to protect intellectual property rights.</i> itm8 has a policy for the protection of intellectual property rights which include the protection of both internally developed intellectual property rights as well as the rights of suppliers, competitors and other relevant parties.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that formal meetings have been scheduled to investigate relevant legislation and regulatory requirements.</p> <p>Based on a sample of meetings, we observed that meetings regarding legal matters have been held.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.33	<p>Protection of records <i>Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release.</i></p> <p>itm8 has established procedures for the protection of records such as log information against loss, destruction, falsification, unauthorised access and unauthorised release which include segregation of duties where employees who have access to delete log data have no access to customer and itm8 systems.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a document management procedure is maintained, reviewed and approved.</p>	No exceptions noted.
5.34	<p>Privacy and protection of personal identifiable information (PII) <i>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.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 has established requirements regarding the preservation of privacy and protection of PII.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.35	<p>Independent review of information security <i>The organisation's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.</i></p> <p>itm8 undergoes regular audits performed by independent external parties, covering both compliance with information security standards and the issuance of assurance reports.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that formal meetings have been scheduled to investigate relevant legislation and regulatory requirements.</p> <p>We inspected that internal audit is performed on the controls.</p>	No exceptions noted.
5.36	<p>Compliance with policies, rules and standards for information security <i>Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.</i></p> <p>itm8 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.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that formal meetings have been scheduled to review the policies, rules, standards etc.</p> <p>From a sample of meetings, we observed that meetings regarding information security have been held.</p>	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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
5.37	<p>Documented operating procedures <i>Operating procedures for information processing facilities shall be documented and made available to personnel who need them.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that operating procedures have been established and that these are subject to updating at least once a year.</p> <p>We furthermore inspected that the operating procedures are accessible to all relevant employees.</p>	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,

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.1	<p>Screening <i>Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis, taking into consideration applicable laws, regulations and ethics, and being proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.</i> itm8 conducts screening of potential candidates, including obtaining clean criminal records for all employees handling customer data. Employees that handle customers data are required to continuously provide a clean criminal record during their employment, which itm8 obtains every three years.</p>	<p>We inquired of 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. We inspected that criminal records have been acquired before employment start.</p>	No exceptions noted.
6.2	<p>Terms and conditions of employment <i>The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security.</i> itm8 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.</p>	<p>We inquired of 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.</p>	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,

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.3	<p>Information security awareness, education and training</p> <p><i>Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training, along with regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.</i></p> <p>itm8 conducts various security awareness initiatives continuously based on an annual plan and emerging security threats. This includes simulations of phishing attempts to enhance employees' hands-on experience. Furthermore, all employees are required to familiarise themselves with applicable information security requirements and the information security policy.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 performs annual security awareness initiatives and performs information security campaigns regularly.</p> <p>We inspected that employees have been introduced to the information security policy.</p>	No exceptions noted.
6.4	<p>Disciplinary process</p> <p><i>A disciplinary process shall be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.</i></p> <p>itm8 has established a formal disciplinary process for violations of information security policies, which is incorporated into all employee contracts.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a formalised procedure is in place which outlines the disciplinary process.</p>	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,

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.5	<p>Responsibilities after termination or change of employment</p> <p><i>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.</i></p> <p>itm8 communicates information security responsibilities that remain in effect after termination or change of employment. This includes obtaining written confirmation that the terminated employee understands their continued obligations.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 obtains a written confirmation of continued obligation after employment from terminated employees.</p>	No exceptions noted.
6.6	<p>Confidentiality or non-disclosure agreements</p> <p><i>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.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that a non-disclosure agreement is signed as part of new employments.</p>	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,

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
6.7	<p>Remote working <i>Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that relevant security measures have been implemented for personnel working remotely.</p> <p>We inspected that remote access from outside of-office locations is enforced through a VPN solution.</p>	No exceptions noted.
6.8	<p>Information security event reporting <i>The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that the incident management process has been communicated and made available to employees.</p>	No exceptions noted.

Control objective 7: Physical controls

Procedures and controls ensure that physical security is implemented and effective.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.1	<p>Physical security perimeters <i>Security perimeters shall be defined and used to protect areas that contain information and other associated assets.</i></p> <p>itm8 has physical security perimeters in place to protect areas containing information and assets, with controls adapted to the relevance and sensitivity of the area.</p>	<p>We made inquiries of Management about the procedures and control activities performed.</p> <p>We observed that itm8 has established appropriate physical security perimeters.</p> <p>We inspected that itm8 has implemented suitable access controls to protect the physical facilities.</p>	No exceptions noted.
7.2	<p>Physical entry <i>Secure areas shall be protected by appropriate entry controls and access points.</i></p> <p>itm8 has established physical entry controls for secure areas, which include identification cards, and constant supervision of approved and cleared employees.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a formal physical access and security policy is maintained, reviewed and approved.</p> <p>We inspected that itm8 has implemented appropriate entry controls to protect physical facilities.</p>	No exceptions noted.
7.3	<p>Securing offices, rooms and facilities <i>Physical security for offices, rooms and facilities shall be designed and implemented.</i></p> <p>itm8 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.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that a formal physical access and security policy is maintained, reviewed and approved.</p> <p>We inspected that itm8 has implemented appropriated entry controls to protect offices, rooms and facilities.</p>	No exceptions noted.
7.4	<p>Physical security monitoring <i>Premises shall be continuously monitored for unauthorised physical access.</i></p> <p>itm8 has established CCTV at all data centres, as well as for selected office buildings based on a risk assessment.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that CCTV is established at entrances to both offices, data centres and other facilities processing sensitive information based on a risk assessment.</p>	No exceptions noted.

Control objective 7: Physical controls

Procedures and controls ensure that physical security is implemented and effective.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.5	<p>Protecting against physical and environmental threats</p> <p><i>Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.</i></p> <p>itm8 has measures in place for secure areas to protect against physical and environmental threats.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that itm8 has designed and implemented measures to protect secure areas against physical and environmental threats.</p> <p>We inspected that appropriate physical and environmental protection measures are in place to safeguard the infrastructure.</p>	No exceptions noted.
7.6	<p>Working in secure areas</p> <p><i>Security measures for working in secure areas shall be designed and implemented.</i></p> <p>itm8 has established procedures and guidelines for working in secure areas to ensure that work performed does not endanger employees or information assets.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that relevant security measures have been established to secure employees and information assets.</p>	No exceptions noted.
7.7	<p>Clear desk and clear screen</p> <p><i>Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that a clear desk and clear screen policy has been implemented.</p>	No exceptions noted.

Control objective 7: Physical controls

Procedures and controls ensure that physical security is implemented and effective.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.8	<p>Equipment siting and protection <i>Equipment shall be sited securely and protected.</i> itm8 has a policy to ensure the protection of critical equipment.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 has established guidelines on the protection against fire, water and heat.</p> <p>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.</p>	No exceptions noted.
7.9	<p>Security of assets off-premises <i>Off-site assets shall be protected.</i> itm8 has established and communicated rules for the protection and handling of assets taken off-premises.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>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.</p>	No exceptions noted.
7.10	<p>Storage media <i>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.</i> itm8 has established and implemented policies and procedures for handling storage media throughout their life cycle.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that itm8 has established and implemented policies and procedures for managing storage media throughout their lifecycle in accordance with the organisation's classification and handling requirements.</p>	No exceptions noted.

Control objective 7: Physical controls

Procedures and controls ensure that physical security is implemented and effective.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.11	<p>Supporting utilities <i>Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.</i> itm8 ensures that all equipment is maintained according to the manufacturer's specifications. Furthermore, itm8 ensures that its partners do the same.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected itm8's own data centre facilities to confirm that appropriate supporting equipment is in place and that such equipment is maintained in accordance with defined maintenance procedures. 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.</p>	No exceptions noted.
7.12	<p>Cabling security <i>Cables carrying power, data, or supporting information services shall be protected from interception, interference or damage.</i> itm8 ensures that cables carrying power, data, or supporting information services are protected according to their sensitivity and is protected as per the manufacturer's recommendations.</p>	<p>We made inquiries of Management about the procedures and control activities performed. We observed that itm8 has implemented measures to protect cabling carrying power, data, and supporting information services in accordance with their sensitivity and manufacturer recommendations. We inspected that cabling protections are in place at relevant datacentres, and that itm8 obtains and reviews assurance reports from hosting providers to ensure requirements are met.</p>	No exceptions noted.
7.13	<p>Equipment maintenance <i>Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.</i> itm8 ensures that equipment is maintained according to the manufacturer's specifications.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected that relevant security measures are implemented to ensure maintenance of equipment.</p>	No exceptions noted.

Control objective 7: Physical controls

Procedures and controls ensure that physical security is implemented and effective.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
7.14	<p>Secure disposal or re-use of equipment <i>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.</i> itm8 has implemented guidelines for the disposal or re-use of equipment, ensuring that storage media is securely destroyed through certified vendors, or that when equipment is returned under warranty or service agreements (e.g., Nutanix without NRDK), any data-bearing components are securely wiped before return.</p>	<p>We made inquiries of Management about the procedures/control activities performed. 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.</p>	<p>No exceptions noted.</p>

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.1	<p>User endpoint devices <i>Information stored on, processed by or accessible via user end point devices shall be protected.</i> itm8 has implemented security policies for user end points, including remote wiping capabilities, malware protection, and other safeguards to ensure adequate protection.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected that itm8 has established and implemented controls for the protection of user end-point devices, including remote wiping capabilities, malware protection and other appropriate safeguards.</p>	No exceptions noted.
8.2	<p>Privileged access rights <i>The allocation and use of privileged access rights shall be restricted and managed.</i> itm8 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.</p>	<p>We inquired of 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.</p>	No exceptions noted.
8.3	<p>Information access restriction <i>Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.</i> itm8 restricts access to systems and applications, ensuring only employees with a work-related need have the necessary permissions.</p>	<p>We inquired of 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.</p>	No exceptions noted.

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.5	<p>Secure authentication <i>Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.</i></p> <p>itm8 has implemented secure authentication technologies for sensitive information, including multi-factor authentication (MFA).</p>	<p>We inspected that a formal access control policy defining allowed technical solutions for authentication is maintained.</p> <p>We inspected that the access control policy has been reviewed and approved.</p> <p>We inspected that access to the customer environment requires the use of multi-factor authentication.</p>	No exceptions noted.
8.6	<p>Capacity management <i>The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that reports on production environment operations at itm8 are sent to customers each month.</p> <p>We furthermore inspected that the capacity of production systems at itm8 is monitored to ensure that future capacity requirements are met.</p>	No exceptions noted.
8.7	<p>Protection against malware <i>Protection against malware shall be implemented and supported by appropriate user awareness.</i></p> <p>itm8 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.</p>	<p>We inquired regarding the procedures/control activities performed.</p> <p>We inspected that antivirus software has been installed on all applicable systems and that antivirus software is monitored.</p> <p>Furthermore, we inspected that user awareness initiatives about antivirus software and malware defence have been established for employees.</p>	No exceptions noted.

Control objective 8: Technological controls

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

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

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.11	<p>Data masking</p> <p><i>Data masking shall be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies and business requirements, taking applicable legislation into consideration.</i></p> <p>itm8 has established procedures for utilising data masking when sensitive data is used for test or development purpose or in general has to leave protected production environments.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We inspected that itm8 has implemented procedures on copying customer data for development and test purposes internally.</p>	No exceptions noted.
8.12	<p>Data leakage prevention</p> <p><i>Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.</i></p> <p>itm8 has established data leakage prevention systems monitoring systems, networks and devices for potential data leakage.</p>	<p>We made inquiries of Management about the procedures/control activities performed.</p> <p>We observed that firewall rules are implemented to restrict access from servers to the internet.</p> <p>We inspected that disk encryption is implemented on user endpoint devices and that such devices are monitored for potential data leakage.</p> <p>We inspected that encryption is implemented for sensitive data stored on servers.</p>	No exceptions noted.
8.13	<p>Information backup</p> <p><i>Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that requirements regarding backup have been established in the contract with subcontractors that provide services where backup is relevant.</p> <p>We inspected that a full restore test of IT environments has been performed.</p>	No exceptions noted.

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.14	<p>Redundancy of information processing facilities <i>Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.</i> itm8 has redundancy in its own information processing facilities and can provide additional redundancy to meet customer requirements.</p>	<p>We inquired of 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.</p>	No exceptions noted.
8.15	<p>Logging <i>Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.</i> itm8 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. Logs cannot be altered. 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.</p>	<p>We inquired of 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.</p>	No exceptions noted.
8.16	<p>Monitoring activities <i>Networks, systems and applications shall be monitored for anomalous behaviour, and appropriate actions taken to evaluate potential information security incidents.</i> itm8 has implemented a monitoring system that ensures customer systems are operational, with alerts for any anomalous behaviour. The system is monitored 24/7.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected that a monitoring system has been implemented and that the system is monitored 24/7.</p>	No exceptions noted.

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.17	<p>Clock synchronisation <i>The clocks of information processing systems used by the organisation shall be synchronised to approved time sources.</i> itm8 has synchronised all relevant information processing systems to a single reference time source.</p>	<p>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.</p>	No exceptions noted.
8.18	<p>Use of privileged utility programs <i>The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.</i> itm8 has established policies for the use of privileged utility programs to ensure that these are not utilised unless a strictly work-related need for them is present.</p>	<p>We made inquiries of Management about the procedures/control activities performed. We observed that connection to servers is done by utilising jump-hosts. We observed that utility programs can only be accessed by a limited number of approved users with a work-related need.</p>	No exceptions noted.
8.19	<p>Installation of software on operational systems <i>Procedures and measures shall be implemented to securely manage software installation on operational systems.</i> itm8 has defined a set of standard implementation descriptions for software installations. These standards are enforced on customer systems to ensure secure management.</p>	<p>We inquired of Management regarding the procedures/control activities performed. We inspected that software installation on operational systems are managed appropriately and according to current procedures.</p>	<p>During our review of one of the selected customers' server environments, it was found that one out of three audited MSSQL servers for the customer had not been sufficiently patched.</p> <p>No further deviations noted.</p>

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.20	<p>Networks security <i>Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.</i> itm8 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.</p>	<p>We inquired regarding the procedures/control activities performed. We inspected whether – in accordance with guidelines – an appropriate security architecture has been established in the network, including whether:</p> <ul style="list-style-type: none"> • 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.
8.21	<p>Security of network services <i>Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.</i> itm8 has identified its security mechanisms, service levels and service requirements of the network service we provide and utilise which is being monitored continuously.</p>	<p>We made inquiries of Management about the procedures/control activities performed. We inspected that an appropriate security architecture has been established in the network.</p>	No exceptions noted.

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.22	<p>Segregation of networks <i>Groups of information services, users and information systems shall be segregated in the organisation's networks.</i></p> <p>itm8 segregates customer networks into one or more networks based on the need for segregation, ensuring that customers cannot access other customer networks.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected the technical security architecture, and whether – in accordance with guidelines – an appropriate security level has been established, including whether:</p> <ul style="list-style-type: none"> • 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.
8.23	<p>Web filtering <i>Access to external websites shall be managed to reduce exposure to malicious content.</i></p> <p>itm8 has implemented web filtering measures to protect against and reduce exposure to malicious content.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that web filtering measures have been implemented.</p>	No exceptions noted.
8.24	<p>Use of cryptography <i>Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.</i></p> <p>itm8 has established policies on the use of cryptography, including rules for usage, selection of cryptographic techniques, implementation, maintenance and disposal.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected that appropriate use of cryptography and cryptographic key management have been established.</p>	No exceptions noted.

Control objective 8: Technological controls

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

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
8.32	<p>Change management <i>Changes to information processing facilities and information systems shall be subject to change management procedures.</i></p> <p>itm8 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.</p>	<p>We inquired of Management regarding the procedures/control activities performed.</p> <p>We inspected the adequacy of change management procedures and inspected that an appropriate change management system is established supported by a technical infrastructure.</p> <p>We inspected that a formal change management procedure has been implemented in the organisation.</p> <p>Using samples, we inspected that the change management procedure is followed.</p>	<p>During our audit, we have found that the existing procedural framework for change management has not been fully comprehensive across all of Managed Services, as different ITSM systems have been used during the period.</p> <p>No further deviations noted.</p>

PENNEO

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

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

Frank Bech Jensen

Kunde

Serienummer: 4ecd2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c

IP: 193.169.xxx.xxx

2026-02-17 12:35:44 UTC



Jesper Parsberg Madsen

PRICEWATERHOUSECOOPERS STATS AUTORISERET

REVISIONSPARTNERSELSKAB CVR: 33771231

Statsautoriseret revisor

Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e

IP: 87.49.xxx.xxx

2026-02-17 12:55:00 UTC



Iraj Bastar

PRICEWATERHOUSECOOPERS STATS AUTORISERET

REVISIONSPARTNERSELSKAB CVR: 33771231

PwC-medunderskriver

Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96

IP: 208.127.xxx.xxx

2026-02-17 13:05:11 UTC



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

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

Sådan kan du verificere, at dokumentet er originalt

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

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