



Assurance report

## IT Forum Gruppen A/S

ISAE 3402 type 2 assurance report on IT general controls for the period 1 January 2025 to 31 December 2025 related to operation of hosting platform

March 2026

Grant Thornton | [www.grantthornton.dk](http://www.grantthornton.dk)  
Lautrupsgade 11, 2100 København Ø  
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | [mail@dk.gt.com](mailto:mail@dk.gt.com)

## Table of contents

Section 1:	IT Forum Gruppen A/S' statement .....	1
Section 2:	Independent service auditor's assurance report on the description of controls, their design and operating effectiveness.....	3
Section 3:	Description of IT Forum Gruppen A/S' services in connection with operating of operation of hosting platform, and related IT general controls .....	5
Section 4:	Control objectives, controls, and service auditor testing .....	13

**Disclaimer:**

The English version of this report was translated from Danish for the convenience of the reader. This translation has not been reviewed or approved by Grant Thornton's auditors. In all legal matters, please refer to the Danish version.

## Section 1: IT Forum Gruppen A/S' statement

The accompanying description has been prepared for customers who have used IT Forum Gruppen A/S' operation of hosting platform, and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

IT Forum Gruppen A/S is using subservice organisations GlobalConnect A/S and Digital Realty Trust Inc. This assurance report is prepared in accordance with the carve-out method and IT Forum Gruppen A/S' description does not include control objectives and controls within GlobalConnect A/S and Digital Realty Trust Inc. Certain control objectives in the description can only be achieved, if the subservice organisation's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control areas, stated in IT Forum Gruppen A/S' description in Section 3 of IT general controls, can only be achieved if the complementary controls with the customers are suitably designed and operationally effective with IT Forum Gruppen A/S' controls. This assurance report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

IT Forum Gruppen A/S confirms that:

- (a) The accompanying description in Section 3 fairly presents the IT general controls related to IT Forum Gruppen A/S' operation of hosting platform processing of customer transactions throughout the period 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:
  - (i) Presents how the system was designed and implemented, including:
    - The type of services provided
    - The procedures within both information technology and manual systems, used to manage IT general controls
    - Relevant control objectives and controls designed to achieve these objectives
    - Controls that we assumed, in the design of the system, 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 along with the specific control objectives that cannot be achieved by us alone
    - Services provided by subservice organisations, including whether they are included according to the inclusive method or the carve-out method
    - Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls
  - (ii) Contains relevant information about changes in the IT general controls, performed during the period from 1 January 2025 to 31 December 2025
  - (iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

- (b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period from 1 January 2025 to 31 December 2025 if relevant controls with the subservice organisation were operationally effective and the customers have performed the complementary controls, assumed in the design of IT Forum Gruppen A/S' controls during the entire 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 used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorisation, during the period from 1 January 2025 to 31 December 2025

Aarhus, 30 March 2026  
IT Forum Gruppen A/S

Mikael Elling  
CEO

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

To IT Forum Gruppen A/S, their customers and their auditors.

### Scope

We have been engaged to report on a) IT Forum Gruppen A/S' description in Section 3 of IT general controls for operation of hosting platform throughout the period from 1 January 2025 to 31 December 2025, and b+c) the design and operational effectiveness of controls related to the control objectives stated in the description.

IT Forum Gruppen A/S is using subservice organisations GlobalConnect A/S and Digital Realty Trust Inc. This assurance report is prepared in accordance with the carve-out method and IT Forum Gruppen A/S' description does not include control objectives and controls within GlobalConnect A/S and Digital Realty Trust Inc. Certain control objectives in the description can only be achieved if the subservice organisation's controls, assumed in the design of our controls, are appropriately designed and operationally effective with the related controls at IT Forum Gruppen A/S..

Some of the control objectives stated in IT Forum Gruppen A/S' description in Section 3 of IT general controls, can only be achieved if the complementary controls with the customers have been appropriately designed and works effectively with the controls with IT Forum Gruppen A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

### IT Forum Gruppen A/S' responsibility

IT Forum Gruppen A/S is responsible for preparing the description in Section 3 and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, IT Forum Gruppen A/S is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

### Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

### Auditor's responsibility

Our responsibility is to express an opinion on IT Forum Gruppen A/S' description (Section 3) as well as on the design and operation of the 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 International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls.

The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation in Section 3.

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

## Limitations of controls at a service organisation

IT Forum Gruppen A/S' description in Section 3, 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 systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

## Opinion

Our opinion has been formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in IT Forum Gruppen A/S' statement in Section 1 and based on this, it is our opinion that:

- (a) the description fairly presents how the IT general controls in relation to IT Forum Gruppen A/S' operation of hosting platform 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 and implemented throughout the period from 1 January 2025 to 31 December 2025 in all material respects, and
- (c) the controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

## Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main Section (Section 4) including control objectives, test, and test results.

## Intended users and purpose

This assurance report is intended only for customers who have used IT Forum Gruppen A/S and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 30 March 2026

### **Grant Thornton**

Godkendt Revisionspartnerselskab

Kristian Randsløv Lydolph  
State Authorised Public Accountant

Andreas Moos  
Partner, CISA, CISM

## Section 3: Description of IT Forum Gruppen A/S' services in connection with operating of operation of hosting platform, and related IT general controls

### Introduction

The following section describes IT Forum Gruppen A/S' services to customers that are covered by the IT general controls addressed in this statement. The statement covers general processes and system configurations, etc., at IT Forum Gruppen A/S.

Processes and system configurations, etc., that are individually agreed upon with IT Forum Gruppen A/S' customers are not covered by this statement. Assessment of any customer-specific processes and system configurations, etc., will be included in specific statements for customers who have ordered such.

### IT Forum Gruppen A/S' services

IT Forum Gruppen A/S provides operations and hosting services to customers with high demands for security, stability, and compliance. The company manages, monitors, and maintains the hosting platform, including networks, servers, and systems, with a strong focus on information security, data integrity, and availability.

### IT Forum Gruppen A/S' information security strategy

IT Forum Gruppen A/S has established a structured and ambitious approach to information security, ensuring that the company's IT services meet the highest standards for security and compliance. The executive management and board of directors continuously prioritise the security level and stay updated on the latest regulatory standards.

### IT Forum Gruppen's transformation and security development

To strengthen its security strategy, IT Forum Gruppen A/S has, over the past year, undergone a comprehensive transformation and implemented a set of security policies that cover all control objectives and strategic security measures. These policies have replaced the previous information security manual and ensure a more flexible and dynamic management of information security. At the same time, the company has transitioned to ISO/IEC 27001:2022, which has resulted in:

- an improved control structure that ensures more effective risk management and threat response
- a proactive approach to cybersecurity and compliance, where security is an integrated part of operations
- increased maturity in security work, where controls and processes have been strengthened.

### Key improvements since last year

Since last year's statement, IT Forum Gruppen A/S has continued the development of its information security and has moved from implementation to a more mature and operationally anchored security and compliance model.

During this period, the company has worked purposefully to consolidate and operationalise its ISMS (Information Security Management System), which has resulted in the following significant improvements:

- **Anchoring of ISMS in operations**  
The ISMS platform is now used as a central management tool for handling controls, risk assessments, and documentation, ensuring systematic and ongoing follow-up on information security.
- **Increased maturity in the control environment**  
The control structure has been further developed and operationalised, strengthening governance, access management, change management, and incident management.

- **Strengthened risk management and ongoing assessment of the threat landscape**  
The risk assessment process has been further developed to support a more dynamic and continuous assessment of risks, enabling a more proactive handling of security threats.
- **Consolidation of the ISO/IEC 27001:2022 framework**  
The transition to ISO/IEC 27001:2022 has been fully implemented and anchored in the organisation's processes, ensuring a modern and robust control foundation.
- **Strengthened compliance and documentation structure**  
Documentation, policies, and controls are continuously maintained and consolidated in a single platform, increasing transparency, traceability, and audit readiness.

Overall, this development supports a higher degree of maturity in IT Forum Gruppen A/S' control environment and ensures that information security is an integrated and ongoing part of the company's operations and governance.

### **Management responsibility and audit**

The board of directors of IT Forum Gruppen receives an annual strategic report on the company's IT security level, including a review of risk profile, security policies, and compliance status. This ensures that management has an updated basis for decision-making.

To support continuous improvement of security measures, ongoing independent assessments of the security level are conducted, as well as an evaluation of the effectiveness of the implemented controls.

These assessments are carried out by a certified IT auditor specialising in IT audit and risk management, ensuring that IT Forum Gruppen's security measures comply with applicable standards and regulatory requirements.

As part of the company's compliance framework, IT Forum Gruppen A/S receives an annual ISAE 3402 assurance report, documenting the company's information security, including control environment, security measures, and operational reliability, thereby strengthening customer transparency and trust in the services provided.

## **IT general controls at IT Forum Gruppen A/S**

The following describes the IT general controls that support IT Forum Gruppen A/S's services to customers, cf. section 1.1.

### **IT controls related to IT hosting services**

IT Forum Gruppen A/S has implemented ISO/IEC 27001:2022 as the basis for its information security controls. The new standard introduces improved risk management, increased resilience, and a modernised approach to cybersecurity and compliance, ensuring a structured and effective management of IT risks.

The description covers the period from 1 January 2025 to 31 December 2025 and is intended solely for IT Forum Gruppen A/S, the company's customers, and their respective auditors.

The most significant security measures include:

- Security policies – Regular updating and review of security policies based on a risk-based approach.
- Organisation of information security – Clearer roles, responsibilities, and management involvement.
- Employee security – Stronger procedures for employee security clearance and increased awareness training.
- Access management – Implementation of Zero Trust principles, stricter access control, and multi-factor authentication (MFA).
- Physical and environmental security – Enhanced security of data centres.
- Operational Reliability – Strengthened monitoring and documented incident management.
- Communications security – Encrypted connections, secure transmission protocols, and advanced network monitoring.
- Management of information security incidents – Structured incident handling and automated alarm systems.
- Contingency management and continuity – Regular testing of contingency plans and emergency procedures.

IT Forum Gruppen A/S performs a number of core tasks for its customers, including:

- The IT operation of customers' solutions is carried out from one or more of IT Forum Gruppen A/S' data centres in Denmark.
- Monitoring of IT operations.
- User support and assistance, including troubleshooting and incident management.

The equipment is owned by IT Forum Gruppen A/S unless otherwise agreed.

IT Forum Gruppen A/S is responsible for implementing and maintaining the necessary security measures in order to prevent and detect errors as well as to ensure compliance with the requirements set out in customer agreements.

### **Subservice organisations**

This statement has been prepared according to the carve-out method and therefore only includes control objectives and associated controls at IT Forum Gruppen but not control objectives and controls at our subcontractors and their subcontractors.

## **Risk management**

IT Forum Gruppen A/S conducts assessments of security risks based on the current threat landscape related to the company's business area – operation and hosting of IT solutions.

The purpose is to ensure that customer data is adequately protected against interruptions, data loss, and unauthorised access – both physically (buildings and supply conditions) and technically (hardware and software) – as well as against internal and external threats, whether intentional or unintentional.

The company continuously assesses the security level – at least once a year and in connection with major system changes – and prioritises necessary measures to maintain a high and up-to-date security level, in accordance with customer requirements and expectations.

Contingency measures have been established to cover both minor and major operational disruptions, with the aim of restoring customers' access to their systems in the data centre as quickly as possible.

The connection between the overall information security strategy and the associated security policies is ensured through close cooperation between executive management and the IT infrastructure manager.

## **Risk handling**

IT Forum Gruppen A/S has integrated risk management into the company's security policies and business processes, so that the identification and handling of risks is a natural part of daily operations.

The executive management and the IT infrastructure manager regularly conduct overall risk and impact assessments, covering buildings, technical infrastructure, applications, business processes, and other critical elements.

The purpose is to ensure that the security level is continuously adapted to changing business needs and the threat landscape – while maintaining a sharp focus on the company's most business-critical systems.

As part of risk management, IT Forum Gruppen A/S has defined and implemented a range of security measures that support stable and secure IT and hosting operations for customers.

## **Organisation of information security**

IT Forum Gruppen A/S has established clear roles and responsibilities for information security, ensuring a structured initiation, management, and control of security processes within the company. These controls support an effective governance structure, where responsibility for information security is clearly defined, distributed, and monitored to ensure compliance with applicable standards and regulatory requirements.

Responsibility for information security is anchored in management and supported by an up-to-date set of security policies, which provide all employees with clear guidelines for behaviour and responsibility. The policies are developed in accordance with ISO/IEC 27001:2022 and are continuously reviewed.

All employees are responsible for protecting information assets and complying with the security policies, which are updated in accordance with ISO/IEC 27001:2022.

All employees are obligated to protect the company's information assets and adhere to applicable security policies. In the event of identified security breaches or threats, employees are required to immediately escalate the incident. All incidents are documented, assessed, and handled in accordance with the established incident management processes.

## Employee security

IT Forum Gruppen A/S has implemented structured controls to ensure that all employees are aware of their responsibility for information security and act in accordance with the company's security policies. This reduces the risk of human error, fraud, and misuse of information assets.

As part of security anchoring, a thorough background assessment is conducted for all candidates prior to employment. This assessment is carried out in accordance with applicable legislation and ethical standards and is adapted to IT Forum Gruppen A/S' security level and risk profile.

Additionally, employees undergo ongoing security training, including annual awareness sessions, to ensure they are updated on the latest threats, risks, and security procedures.

## Access management

IT Forum Gruppen A/S has established reliable controls to ensure that access to systems, data, and networks is managed in accordance with business and legal requirements. The controls are designed to protect the company's IT environment against unauthorised access and potential security risks.

IT Forum Gruppen A/S has established guidelines for access management that define access rules and rights for users or groups of users. This access management includes both logical and physical access, which is granted based on work-related needs.

All customers who require access to systems in primary operations must have explicitly defined logins, which are validated centrally. Upon login, automatic logging of the user occurs.

IT Forum Gruppen A/S' employees are defined centrally, from where login to servers is validated. When logging into a server, audit/logging must be performed. Servers and other central equipment, where it is not possible to comply with the above, must have the access control to the system described in the operational documentation.

All users at IT Forum Gruppen A/S are assigned a unique identity for personal use. Upon employment, employees sign that their personal codes are confidential and that any group access codes may only be known by the company's employees.

Default access codes from system suppliers are changed after system installation.

In cases where extended access rights are needed, they are granted to the extent deemed necessary for the execution of a given task. After the task is completed, the extended access rights must be revoked.

If extended access rights are allowed for longer periods (longer than until the end of the working day), the operations manager must be notified in writing.

Access rights for the company's employees are reviewed once a year and reassessed in connection with changes in the employee's work-related circumstances. Approvals for extended access rights must be regularly reviewed to ensure that access rights correspond to the individual's actual needs.

In the event of resignation, the employee's manager assesses the employee's rights to the information system and revokes them if necessary. The employee's data files and emails are reviewed as soon as possible, and relevant content is transferred to other employees. The logon procedure must minimise the possibilities for unauthorised access by revealing as little as possible about the system.

## Physical and environmental security

IT Forum Gruppen A/S has implemented robust controls to ensure that critical information assets are protected against physical threats, unauthorised access, and environmental risks. Reliable controls have been established to ensure that:

- Critical information assets are protected against unauthorised physical access, damage, and disruptions.
- Information processing equipment and storage media are kept in secure areas with necessary barriers and access control.
- The risk of loss, damage, or compromise of information assets is minimised through strict security measures.
- Equipment is effectively protected against physical threats, including theft, sabotage, and environmental impacts.
- Power supply, ventilation, and cable installations are adequate and secured against operational disruptions.

### Physical security in data centres

IT Forum Gruppen A/S' primary data centres have a high level of security, capable of withstanding civil sabotage attempts, unauthorised intrusion, theft, and vandalism. This includes:

- Building security measures such as shielded windows, double steel doors, and alarm systems.
- In the event of a break-in, the alarm centre is activated immediately, and the company's contingency procedure is initiated.
- Access to primary data centres is limited to authorised operations technicians, and all physical access is logged for traceability.

External consultants, craftsmen, and cleaning staff may only gain access when accompanied by an authorised operations technician. For longer-term work, external personnel may be granted temporary access, provided they have signed a confidentiality agreement.

### Data protection and redundancy

- Customers' business-critical data is backed up at least daily and stored in encrypted form at secondary data centres to ensure recovery options.
- Cooling systems are redundant according to the N+1 principle, meaning that any single component can fail without affecting operations. Fan coils with fans and heat exchangers ensure a stable temperature in the operational area.
- Fire protection safeguards against both internal and external fires – No hazardous or flammable materials are stored in the same rooms as the data centres. Automatic fireproof doors ensure containment in the event of a fire. An Inergen-based automatic fire extinguishing system is installed in the operational area.

### Power supply and network security

- Primary data centres are connected to a buried power cable, ensuring a stable supply.
- There is UPS power backup, which protects against transients and ensures sufficient time for shutdown in the event of a power failure.
- Emergency power systems are tested annually, and the diesel generator is started quarterly to ensure operational readiness.

The data centres also have redundant telecommunications connections, which exit the building through different entry points to ensure continued availability in the event of an outage.

### **Cable security and workstations**

- Cables in data centres are protected against pulling and breakage via cable trays and ducts.
- Cables in the core network are labelled with relevant information, and penetrations in masonry and floor separations are fireproofed with fire-retardant material.
- Documentation for network cabling is continuously updated to ensure overview and maintenance.
- Workstations and systems in primary operational systems are configured to automatically lock the screen and keyboard after 15 minutes of inactivity or manually when leaving the workstation.

This comprehensive physical and environmental security ensures that IT Forum Gruppen A/S's infrastructure remains resilient, stable, and secure in all scenarios.

### **Physical and environmental security – service subservice organisations**

This statement has been prepared according to the partial method and therefore only includes control objectives and associated controls at IT Forum Gruppen A/S but not control objectives and controls at our subsuppliers and their subsuppliers.

### **Operational reliability**

IT Forum Gruppen A/S has established reliable controls to ensure that systems and data are properly backed up and can be restored.

There are security policies and operational documentation in place to ensure that any operations technician is able to resolve issues up to a total system failure. The operational documentation is updated upon changes. In case of errors, contact persons are appointed to handle customer communications, while operations technicians resolve the issues.

Major changes in software and hardware must be planned and documented in sufficient detail, including an assessment of the impact of the change. In addition, emergency procedures are documented in case of failed changes. If deemed necessary, changes must be tested before being put into production.

Server and service capacity is measured and monitored regularly to ensure sufficient capacity. Alarms are triggered when capacity limits are exceeded.

System-level separation between environments is established when deemed necessary in specific customer cases. Where such separation is implemented, all relevant units will be marked. Only designated employees have access to this environment. This separation is also used in development contexts to ensure clear differentiation between test and production environments.

Servers are installed with up-to-date antivirus software.

Daily backups are taken of the core IT infrastructure. The backup is stored in encrypted form at a secondary location. To meet customer requirements for data security and data recovery in the data centre, daily backups are made of both the customer's business-critical data and the servers that the customer has placed in the data centre. Backups are stored as standard for at least 28 versions back. Recovery procedures are regularly tested on backups by restoring selected files for customers.

User activities, deviations, and security incidents are logged and stored for a defined period to support follow-up on access controls and possible investigation of errors and misuse. The use of IT Forum's primary operational systems is monitored and followed up on an ongoing basis. The level of monitoring is determined based on a risk assessment and legal requirements. Errors in primary operational systems are logged and analysed, and necessary corrections and countermeasures are implemented. Log facilities and log information are protected against manipulation. Activities performed by system administrators and operators, as well as others with special privileges, are logged.

There are business procedures for the installation of systems in operational environments.

## Communications security

IT Forum Gruppen A/S has established reliable controls to ensure correct and secure data communication between the company's systems, customers, and partners. Guidelines and procedures have been defined to protect information exchange and communication against threats and unauthorised access.

The company's network is structured and segmented so that internal and external systems are separated to minimise the risk of compromise. Network traffic is continuously monitored, and advanced security solutions, including firewalls, Intrusion Prevention Systems (IPS), and web filtering, ensure that all data exchange is controlled and protected.

IT Forum Gruppen A/S uses encryption and secure communication protocols to protect data during transmission. Critical networks and wireless connections are secured through access control and monitoring, while external network interfaces are configured to reject all unknown traffic by default.

Collaboration with third-party vendors is supported by contractual security requirements, including requirements for compliance with relevant standards and certifications such as ISAE 3402. The IT Security team is responsible for ensuring that the network architecture is continuously evaluated and optimised in accordance with best practices and the company's risk assessments.

Through this proactive approach to communications security, IT Forum Gruppen A/S ensures a robust and scalable network infrastructure that protects business-critical systems and data against modern security threats.

## Management of subservice organisations

IT Forum Gruppen A/S has established reliable controls to ensure that written cooperation agreements are in place with relevant suppliers.

Agreements for cooperation with relevant suppliers are entered into after management has conducted a security assessment.

IT Forum Gruppen maintains close dialogue with the subservice organisation and receives an ISAE 3402 assurance report or an equivalent statement from the subservice organisation.

## Management of information security incidents

IT Forum Gruppen A/S has established a structured and documented process for handling information security incidents, ensuring timely identification, reporting, and remediation. The purpose is to minimise risks, reduce the consequences of security breaches, and continuously improve the company's security measures.

The company has a dedicated policy and internal guidelines that set out procedures for follow-up on IT security incidents. These incidents are registered and documented in relevant systems, where they are followed up and evaluated to ensure a structured and transparent handling.

Incidents are managed by the operations manager in collaboration with the IT Security team, where an assessment of the severity of the incident is carried out. Necessary corrective actions are initiated immediately, and guidelines for preventive measures are prepared.

After handling, the incident is evaluated, experiences are documented, and improvements to processes and controls are implemented to reduce the likelihood of recurrence.

This systematic approach to security incidents ensures that IT Forum Gruppen A/S can respond quickly and effectively to threats, while also ensuring the continuous improvement of information security.

## Contingency management

IT Forum Gruppen A/S has established structured and well-defined controls to ensure continued operations and rapid recovery in the event of system failures or disasters. The purpose is to minimise business disruptions, protect critical processes, and ensure the timely restoration of the company's operations.

As part of the company's business continuity strategy, ongoing risk assessments of critical systems and processes are conducted. Identified risks are prioritised and documented, providing a dynamic overview of the company's security model and potential vulnerabilities.

To ensure a swift and effective recovery, contingency and recovery plans have been prepared, setting out procedures for the maintenance and restoration of operations within a defined timeframe following a disruption.

These plans are tested at least once a year, during which their relevance and effectiveness are evaluated. The results are documented in an evaluation report, which forms the basis for any improvements and optimisations of the contingency strategy.

This systematic approach to contingency management ensures that IT Forum Gruppen A/S can respond quickly and effectively to incidents, while the company's critical functions are maintained and remain protected against major disruptions.

## Significant changes in IT general controls

There have been no significant changes in the IT general controls during the audit period.

## Complementary controls at the customers

Customers are responsible for data transmission between IT Forum Gruppen A/S and the customer. It is therefore the customers' responsibility to ensure controls in this regard.

Furthermore, all user administration, including the assignment of rights and protection of access via equipment located at the customers' premises, is the responsibility of the customer. Customers must therefore control all user administration.

The procurement, development, and implementation of business systems and user systems are the responsibility of the customers. Controls regarding system development, procurement, and change management are the customers' responsibility.

Access to business systems and user systems is the responsibility of the customers. Controls regarding access to these systems and their data are the customers' responsibility.

Each customer, as the data controller, must enter into a contract with IT Forum Gruppen as the data processor, which must ensure that IT Forum Gruppen acts solely on the instructions of the individual customer, and that IT Forum Gruppen takes all necessary technical and organisational security measures for the processing of personal data.

## Section 4: Control objectives, controls, and service auditor testing

### Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This statement is issued according to the carve-out method and therefore does not include controls of IT Forum Gruppen A/S' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by IT Forum Gruppen A/S' customers, are not included in this report.

### Tests performed

We performed our test of controls at IT Forum Gruppen A/S, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at IT Forum Gruppen A/S regarding controls. Inquiries have included questions on how controls are being performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

## Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with IT Forum Gruppen A/S.

<b>A.5 Organisational controls</b>			
<b>Control objective: To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.</b>			
<b>No.</b>	<b>IT Forum Gruppen A/S' control</b>	<b>Grant Thornton's test</b>	<b>Test results</b>
5.1	<p><i>Policies for information security</i></p> <p>Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.</p>	<p>We have inspected that there is a formal, written, and identifiable information security policy, which has been approved by the company's management.</p> <p>We have inspected that the information security policy has been published and communicated to the employees, and that it has been updated within the audit period.</p>	No deviations noted.
5.2	<p><i>Information security roles and responsibilities</i></p> <p>Information security roles and responsibilities should be defined and allocated according to the organisation's needs.</p>	<p>We have inspected that roles and responsibilities for information security are formally defined and documented within the organisation, and that these are updated and applicable for the audit period.</p> <p>We have inspected that roles and responsibilities are allocated to named individuals or functions within the organisation.</p> <p>We have inspected the organisational chart to verify that responsibility for information security is clearly indicated and can be identified within the organisation's structure.</p>	No deviations noted.

<b>No.</b>	<b><i>IT Forum Gruppen A/S' control</i></b>	<b><i>Grant Thornton's test</i></b>	<b><i>Test results</i></b>
5.3	<p><i>Segregation of duties</i></p> <p>Conflicting duties and conflicting areas of responsibilities should be segregated.</p>	<p>We have inspected that segregation of duties is documented and formalised through the organisational chart with clear roles, names, and reporting lines.</p> <p>We have inspected documentation describing the allocation of specific roles and rights, as well as the segregation of conflicting tasks and areas of responsibility.</p> <p>We have inspected that the organisational chart has been updated within the audit period, and that segregation of duties is implemented and documented through distinct roles within the organisation.</p>	No deviations noted.
5.4	<p><i>Management responsibilities</i></p> <p>Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and the organisation's procedures.</p>	<p>We have inspected that management has established and formally approved an information security policy for the organisation.</p> <p>We have inspected that the organisation's procedures require employees to comply with information security policies and procedures.</p> <p>We have inspected that employment contracts include requirements for compliance with the organisation's information security policies and procedures.</p> <p>We have, by sample test, inspected that the requirements for compliance with information security measures are included in employees' employment contracts.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To establish a management framework that ensures the identification and mitigation of information security risks related to legal, regulatory, supervisory authorities, threats and project management.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.5	<p><i>Contact with authorities</i></p> <p>The organisation should establish and maintain contact with relevant authorities.</p>	<p>We have inspected that a procedure has been established for contact with relevant authorities, and that the organisation has identified the relevant authorities, including supervisory bodies and agencies.</p> <p>We have inspected documentation for the maintenance and updating of the procedure for contact with authorities during the audit period.</p>	No deviations noted.
5.6	<p><i>Contact with special interest groups</i></p> <p>The organisation should establish and maintain contact with special interest groups or other specialist security forums and professional associations.</p>	<p>We have inspected documentation that a documented procedure exists for contact with special interest groups, and that this procedure has been followed during the audit period.</p> <p>We have inspected documentation that there has been contact with interest groups during the audit period.</p>	No deviations noted.
5.7	<p><i>Threat intelligence</i></p> <p>Information relating to information security threats should be gathered and analysed to establish threat intelligence.</p>	<p>We have inspected that procedures for handling and analysing threats are documented, approved, and allocate responsibilities and methods.</p> <p>We have inspected that the collection and analysis of threats have been carried out and documented during the period.</p>	No deviations noted.
5.8	<p><i>Information security in project management</i></p> <p>Information security should be integrated into project management.</p>	<p>We have inspected that there is documentation for the integration of information security principles in the project management process, including risk assessments and the involvement of the information security manager.</p> <p>We have inspected an overview of projects carried out during the period with relevant information.</p> <p>We have, by sample test, inspected that information security requirements have been integrated into specific projects.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To identify organisational assets and define appropriate areas of responsibilities for protection hereof.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.9	<p><i>Inventory of information and other associated assets</i></p> <p>An inventory of information and other associated assets, including owners, should be developed and maintained.</p>	<p>We have inspected that a register of information and supporting assets has been prepared, including owners and classification, with ongoing maintenance and documented responsibility.</p> <p>We have inspected that the register of information and supporting assets has been updated during the audit period.</p> <p>We have inspected that ownership is indicated for assets in the register in practice.</p>	No deviations noted.
5.10	<p><i>Acceptable use of information and other associated assets</i></p> <p>Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.</p>	<p>We have inspected that a procedure for acceptable use of information and assets has been prepared.</p> <p>We have inspected that the rules for acceptable use of information and assets have been implemented.</p>	No deviations noted.
5.11	<p><i>Return of assets</i></p> <p>Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.</p>	<p>We have inspected a documented procedure for the return of assets upon termination of employment, where responsibilities are clearly allocated to the immediate manager and the IT department.</p> <p>We have inspected a list of employees who have left during the period.</p> <p>We have, by sample test, inspected documentation that employees who have left have returned the organisation's assets.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.12	<p><i>Classification of information</i></p> <p>Information should be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements.</p>	<p>We have inspected the procedure for classification of information and assets.</p> <p>We have inspected examples of classified information, where the classification has been carried out in accordance with the documented procedure, with indication of classification levels and clear allocation of responsibilities.</p>	No deviations noted.
5.14	<p><i>Information transfer</i></p> <p>Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties.</p>	<p>We have inspected the procedure for the transfer of information.</p> <p>We have inspected that security protocols are implemented, including the use of encrypted services, TLS encryption, access control, monitoring, and logging.</p> <p>We have inspected that encrypted or approved transfer services are used when transferring sensitive information, and that this can be documented through specific examples as well as annual reviews of procedures and confidentiality requirements.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To ensure authorised access and to prevent unauthorised access to information and other associated assets.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.15	<p><i>Access control</i></p> <p>Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.</p>	<p>We have inspected that a procedure for access management exists.</p> <p>We have inspected that the procedure for access management includes a documented update date.</p>	No deviations noted.
5.16	<p><i>Identity management</i></p> <p>The full life cycle of identities should be managed.</p>	<p>We have inspected documentation for procedures for managing the lifecycle of identities.</p> <p>We have inspected that users are assigned a unique user ID upon creation, and that user rights are allocated based on job function and defined roles.</p> <p>We have, by sample test, inspected that the allocation of user rights is approved by the immediate manager, and that users are created with unique user IDs and rights in accordance with their job function.</p>	No deviations noted.
5.17	<p><i>Authentication information</i></p> <p>Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.</p>	<p>We have inspected that a written procedure for the management of authentication information exists.</p> <p>We have inspected documentation showing that the password configuration in the system meets the requirements for minimum length, complexity, history, and expiry in accordance with the documented procedure for access management.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.18	<p><i>Access rights</i></p> <p>Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.</p>	<p>We have inspected procedures for the assignment, modification, and removal of access rights.</p> <p>We have inspected that a process has been established for the timely removal of access rights upon termination of employment.</p> <p>We have, by sample test, inspected documentation that the assignment of user rights is approved by the immediate manager, that users are created with unique user IDs, and that rights are allocated in accordance with their job function.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To maintain an agreed level of information security in supplier relationships and service delivery in line with supplier agreements.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.19	<p><i>Information security in supplier relationships</i></p> <p>Processes and procedures should be defined and implemented to manage the information security risks, associated with the use of supplier's products or services.</p>	<p>We have inspected the procedure for the management of supplier relationships and service agreements.</p> <p>We have inspected documentation that ongoing control, risk assessment, and monitoring have been established, and that no exceptions have been identified during the review.</p>	No deviations noted.
5.21	<p><i>Managing information security in the ICT supply chain</i></p> <p>Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.</p>	<p>We have inspected the procedure for managing information security risks in the supply chain for ICT products and services.</p> <p>We have inspected that the procedure describes the identification and handling of information security risks in the supply chain.</p> <p>We have inspected that the procedure has been updated within the audit period and approved by the relevant responsible parties with a documented approval date.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.22	<p><i>Monitoring, review and change management of supplier services</i></p> <p>The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.</p>	<p>We have inspected that processes for monitoring, assessment, and change management of supplier services have been established and documented.</p> <p>We have inspected that monitoring, risk assessment, and follow-up on significant risks have been carried out during the audit period for all key suppliers.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To ensure a quick, effective, consistent and orderly approach to the management of information security incidents, including communication on security events and weaknesses.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.24	<p><i>Information security incident management planning and preparation</i></p> <p>The organisation should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.</p>	<p>We have inspected that a formal procedure exists for the planning and preparation of incident management in the event of security incidents.</p> <p>We have inspected that information about roles and responsibilities has been made available to relevant employees via the organisation's intranet.</p>	No deviations noted.
5.25	<p><i>Assessment and decision on information security events</i></p> <p>The organisation should assess information security events and decide if they are to be categorised as information security incidents.</p>	<p>We have inspected that a formal, written, and management-approved procedure exists for the assessment and decision-making regarding information security incidents, and that this has been communicated to relevant employees.</p> <p>We have, by sample test, inspected that information security incidents have been categorised in accordance with the procedure.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.26	<p><i>Response to information security incidents</i></p> <p>Information security incidents should be responded to in accordance with the documented procedures.</p>	<p>We have inspected that a documented, formal, and approved procedure exists for the handling of information security incidents.</p> <p>We have, by sample test, inspected that information security incidents have been handled in accordance with the procedure.</p>	No deviations noted.
5.27	<p><i>Learning from information security incidents</i></p> <p>Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.</p>	<p>We have inspected that a documented procedure exists for learning from information security incidents.</p> <p>We have, by sample test, inspected that security incidents have been recorded in order to reduce the risk of recurrence.</p>	No deviations noted.
5.28	<p><i>Collection of evidence</i></p> <p>The organisation should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.</p>	<p>We have inspected that a written and version-controlled procedure exists for the collection of evidence in the event of information security incidents.</p> <p>We have, by sample test, inspected that evidence has been identified, collected, and stored in accordance with the procedure.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.29	<p><i>Information security during disruption</i></p> <p>The organisation should plan how to maintain information security at an appropriate level during disruption.</p>	<p>We have inspected that information security continuity is embedded in the organisation's contingency plans through documentation of the preparation, approval, and availability of the plans for relevant employees.</p> <p>We have inspected that contingency exercises involving crisis management and relevant roles have been carried out, and that test activities have been documented and evaluated.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To ensure the protection and availability of information and other associated assets during disruption.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.30	<p><i>ICT readiness for business continuity</i></p> <p>ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.</p>	<p>We have inspected that the Business Impact Analysis (BIA) is documented, dated, and approved.</p> <p>We have inspected that RTO and RPO have been established.</p> <p>We have inspected that contingency plans and related policies have been tested and evaluated through contingency exercises, where both technical and organisational aspects as well as compliance with RTO and RPO are documented.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To ensure compliance with and avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.31	<p><i>Legal, statutory, regulatory and contractual requirements</i></p> <p>Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements should be identified, documented and kept up to date.</p>	<p>We have inspected that a register of legal, statutory, regulatory, and contractual requirements relevant to information security has been prepared, and that the organisation's approach to handling these requirements is documented.</p> <p>We have inspected that the organisation's approach to handling relevant requirements is continuously updated through annual review.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.32	<p><i>Intellectual property rights</i></p> <p>The organisation should implement appropriate procedures to protect intellectual property rights.</p>	<p>We have inspected documented procedures for the protection of intellectual property rights.</p> <p>We have inspected that access to critical copyrights (e.g. source codes) has been restricted to employees with a work-related need.</p>	No deviations noted.
5.33	<p><i>Protection of records</i></p> <p>Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release.</p>	<p>We have inspected that procedures have been defined for the protection of records against loss, destruction, falsification, unauthorised access, and disclosure.</p> <p>We have inspected documentation for the implementation of immutable backup of logs.</p>	No deviations noted.
5.34	<p><i>Privacy and protection of PII</i></p> <p>The organisation should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.</p>	<p>We have inspected that internal controls exist for the storage and deletion of personal data as well as overall policies and frameworks for the protection of PII, and that internal controls related to the protection of personal data are documented.</p>	No deviations noted.

## A.5 Organisational controls

Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.36	<p><i>Compliance with policies, rules and standards for information security</i></p> <p>Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed.</p>	<p>We have inspected that information security is implemented and operational in accordance with the organisational measures and procedures.</p> <p>We have inspected a detailed overview of internal controls related to information security.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
5.37	<p><i>Documented operating procedures</i></p> <p>Operating procedures for information processing facilities should be documented and made available to personnel who need them.</p>	<p>We have inspected that the operational procedures are version-controlled, dated, and approved.</p> <p>We have inspected documentation for formal and approved operational procedures for information processing facilities.</p>	No deviations noted.

## A.6 People controls

Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
6.1	<p><i>Screening</i></p> <p>Background verification checks on all potential candidates should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.</p>	<p>We have inspected that a documented and approved procedure for screening new employees exists.</p> <p>We have, by sample test, inspected that background checks of new employees have been carried out in accordance with the procedure.</p>	No deviations noted.
6.2	<p><i>Terms and conditions of employment</i></p> <p>The employment contractual agreements should state the personnel's and the organisation's responsibilities for information security.</p>	<p>We have, by sample test, inspected that signed employment contracts describe the responsibilities of the employee and the organisation regarding information security.</p>	No deviations noted.

## A.6 People controls

Control objective: To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities as well as understand the consequences of information security policy violations.

<b>No.</b>	<b>IT Forum Gruppen A/S' control</b>	<b>Grant Thornton's test</b>	<b>Test results</b>
6.3	<p><i>Information security awareness, education and training</i></p> <p>The organisation's personnel and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.</p>	<p>We have inspected that a formal information security awareness programme has been established, which is risk-based, role-specific, and includes annual training.</p> <p>We have inspected that the awareness programme covers relevant topics regarding the organisation's information security policies and procedures.</p> <p>We have inspected that updates to information security policies and procedures are communicated to employees via email-based training modules and awareness campaigns.</p> <p>We have inspected documentation for the completion of information security training, including records of employee participation.</p>	No deviations noted.
6.4	<p><i>Disciplinary process</i></p> <p>A disciplinary process should be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.</p>	<p>We have inspected that a formal and documented sanctions process exists for breaches of the information security policy.</p> <p>We have, by sample test, inspected that signed employment contracts include the sanctions process.</p>	No deviations noted.

## A.6 People controls

Control objective: To protect the organisation's interests as part of the process of changing or terminating employment

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
6.5	<p><i>Responsibilities after termination or change of employment</i></p> <p>Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.</p>	<p>We have inspected that information security responsibilities and obligations after termination or change of employment are clearly defined, and that the documentation specifies which employees and roles are subject to these obligations.</p> <p>We have, by sample test, inspected that employees who have left have been informed that information security responsibilities and obligations remain in effect after the termination of employment.</p>	No deviations noted.
6.6	<p><i>Confidentiality or non-disclosure agreements</i></p> <p>Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.</p>	<p>We have inspected that a formal and documented confidentiality agreement exists.</p> <p>We have, by sample test, inspected signed confidentiality agreements for external parties.</p> <p>We have, by sample test, inspected that confidentiality agreements have been signed by employees.</p>	No deviations noted.

## A.6 People controls

Control objective: To ensure an adequate level of security when personnel are working remotely and an effective reporting of information security events.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
6.7	<p><i>Remote working</i></p> <p>Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.</p>	<p>We have inspected that documented security requirements for remote work exist, including requirements for firewall rules, VPN, and technical requirements for equipment.</p> <p>We have inspected documentation that multi-factor authentication has been implemented.</p> <p>We have inspected documentation that VPN is used for secure communication during remote work, including firewall rules, logs, and VPN configurations.</p>	No deviations noted.
6.8	<p><i>Information security event reporting</i></p> <p>The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.</p>	<p>We have inspected that a formal and approved procedure for reporting information security incidents exists.</p> <p>We have inspected that employees have access to the procedure for reporting information security incidents and use relevant channels for reporting information security incidents.</p>	No deviations noted.

## A.7 Physical controls

Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and other associated assets.

<b>No.</b>	<b>IT Forum Gruppen A/S' control</b>	<b>Grant Thornton's test</b>	<b>Test results</b>
7.1	<p><i>Physical security perimeters</i></p> <p>Security perimeters should be defined and used to protect areas that contain information and other associated assets.</p>	<p>We have inspected that procedures for physical area security are documented and approved.</p> <p>We have inspected the implementation of these physical security measures and access control at relevant locations.</p>	No deviations noted.
7.2	<p><i>Physical entry</i></p> <p>Secure areas should be protected by appropriate entry controls and access points.</p>	<p>We have inspected the procedure for the assignment and removal of physical access to secured areas.</p> <p>We have inspected that access rights to secured areas are reviewed quarterly, and that log reviews have been carried out during the period.</p>	No deviations noted.
7.3	<p><i>Securing offices, rooms and facilities</i></p> <p>Physical security for offices, rooms and facilities should be designed and implemented.</p>	<p>We have inspected that physical security measures are implemented and documented.</p>	No deviations noted.
7.5	<p><i>Protecting against physical and environmental threats</i></p> <p>Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.</p>	<p>We have inspected that written procedures for protection against physical and environmental threats have been established and approved by management.</p> <p>We have inspected that fire extinguishing equipment as well as fire and smoke alarms have been installed in critical areas, and that leakage alarm tests for the detection of moisture and water have been carried out.</p>	No deviations noted.
7.6	<p><i>Working in secure areas</i></p> <p>Security measures for working in secure areas should be designed and implemented.</p>	<p>We have inspected procedures for work in secured areas.</p> <p>We have inspected that access control, access logs, monitoring, and access restrictions are implemented in secured areas, including that physical security measures are only accessible to authorised employees.</p>	No deviations noted.

## A.7 Physical controls

Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
7.8	<p><i>Equipment siting and protection</i></p> <p>Equipment should be sited securely and protected.</p>	<p>We have inspected the procedure for the placement and protection of equipment.</p> <p>We have inspected documentation that access to secured areas is controlled via access control, including key fobs and locking systems.</p>	No deviations noted.
7.10	<p><i>Storage media</i></p> <p>Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.</p>	<p>We have inspected the procedure for the management of storage media.</p> <p>We have inspected documentation for the handling of storage media in accordance with the procedure.</p> <p>We have inspected documentation for the disposal of storage media.</p>	No deviations noted.
7.11	<p><i>Supporting utilities</i></p> <p>Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.</p>	<p>We have inspected documented procedures for the protection of information processing equipment against power failure and other disruptions.</p> <p>We have, by sample test, inspected service inspections of UPS and generator.</p>	No deviations noted.
7.12	<p><i>Cabling security</i></p> <p>Cables carrying power, data or supporting information services should be protected from interception, interference or damage.</p>	<p>We have inspected documented procedures and policies for the protection of cables.</p> <p>We have inspected documentation showing that cables are protected.</p>	No deviations noted.
7.13	<p><i>Equipment maintenance</i></p> <p>Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.</p>	<p>We have inspected the procedure for equipment maintenance.</p> <p>We have inspected documentation for maintenance carried out on equipment.</p>	No deviations noted.

<b>No.</b>	<b>IT Forum Gruppen A/S' control</b>	<b>Grant Thornton's test</b>	<b>Test results</b>
7.14	<p><i>Secure disposal or re-use of equipment</i></p> <p>Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.</p>	<p>We have inspected that a documented procedure exists for the deletion and destruction of data on storage media prior to disposal or reuse.</p> <p>We have inspected documentation for disposed equipment.</p>	No deviations noted.

## A.8 Technological controls

Control objective: To protect information against the risks introduced by using user endpoint devices.

<b>No.</b>	<b>IT Forum Gruppen A/S' control</b>	<b>Grant Thornton's test</b>	<b>Test results</b>
8.1	<p><i>User endpoint devices</i></p> <p>Information stored on, processed by or accessible via user endpoint devices should be protected.</p>	<p>We have inspected the procedure for the management of mobile devices.</p> <p>We have inspected that the policy for the use of mobile devices has been made available to relevant employees.</p> <p>We have inspected that the installation of software on user equipment is technically restricted.</p> <p>We have inspected that anti-malware software has been implemented on laptops.</p>	No deviations noted.

## A.8 Technological controls

Control objective: To ensure that the allocation and use of privileged access rights have been restricted and controlled to reduce the risk of unauthorised access, changes to systems and inaccurate authentication.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.2	<p><i>Privileged access rights</i></p> <p>The allocation and use of privileged access rights should be restricted and managed.</p>	<p>We have inspected the procedure for the administration of privileged access rights.</p> <p>We have inspected that privileged access rights are only granted based on work-related needs, and that the need is continuously validated.</p>	No deviations noted.
8.3	<p><i>Information access restriction</i></p> <p>Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.</p>	<p>We have inspected the policy for access management.</p> <p>We have inspected that the allocation of user rights is based on documented user groups and roles.</p> <p>We have inspected that criteria for access to sensitive data are established and documented, including role, department, tasks, and approval.</p> <p>We have inspected documentation for the approval of access rights.</p>	No deviations noted.
8.4	<p><i>Access to source code</i></p> <p>Read and write access to source code, development tools and software libraries should be appropriately managed.</p>	<p>We have inspected that the assignment and use of privileged access rights to source code are controlled and restricted.</p> <p>We have inspected that access to source code is limited to authorised individuals through access control mechanisms.</p>	No deviations noted.
8.5	<p><i>Secure authentication</i></p> <p>Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.</p>	<p>We have inspected that a procedure for password management has been established.</p> <p>We have inspected documentation for password configurations, including minimum length, complexity requirements, password memory, maximum lifetime, lockout functionality, and requirements for mobile devices.</p> <p>We have inspected documentation for the implementation and use of multi-factor authentication on relevant systems.</p>	No deviations noted.

## A.8 Technological controls

Control objective: To ensure correct and secure operation of information processing facilities.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.6	<p><i>Capacity management</i></p> <p>The use of resources should be monitored and adjusted in line with current and expected capacity requirements.</p>	<p>We have inspected that procedures for the monitoring of information processing resources have been specified.</p> <p>We have inspected documentation for the implementation of technical solutions for monitoring, which support the ongoing monitoring of resources and capacity.</p>	No deviations noted.
8.7	<p><i>Protection against malware</i></p> <p>Protection against malware should be implemented and supported by appropriate user awareness.</p>	<p>We have inspected the procedure for protection against malware.</p> <p>We have inspected system reports and documentation showing that anti-malware software is installed, active, and updated.</p>	No deviations noted.
8.8	<p><i>Management of technical vulnerabilities</i></p> <p>Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be assessed and appropriate measures should be taken.</p>	<p>We have inspected the procedure for the management of technical vulnerabilities.</p> <p>We have inspected documentation for daily and weekly vulnerability scans, response to identified vulnerabilities, and the handling of deviations in accordance with the procedure.</p>	No deviations noted.
8.9	<p><i>Configuration management</i></p> <p>Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.</p>	<p>We have inspected that documented and version-controlled baseline security configurations are in place.</p> <p>We have inspected that processes for configuration management have been established.</p> <p>We have inspected that procedures and tools for monitoring and assessing security configurations have been established.</p> <p>We have inspected documentation for implemented configuration management, including patching, security configurations, encryption, compliance controls, endpoint policies, and the registration and monitoring of hardware and software.</p>	No deviations noted.

## A. 8 Technological controls

Control objective: To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements.

<b>No.</b>	<b><i>IT Forum Gruppen A/S' control</i></b>	<b><i>Grant Thornton's test</i></b>	<b><i>Test results</i></b>
8.10	<p><i>Information deletion</i></p> <p>Information stored in information systems, devices or in any other storage media should be deleted when no longer required.</p>	<p>We have inspected the procedure for the deletion of information.</p> <p>We have inspected documentation showing that information systems are configured for the automatic deletion of information.</p> <p>We have inspected documentation showing that automatic deletion functions have been used during the period.</p>	No deviations noted.
8.12	<p><i>Data leakage prevention</i></p> <p>Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.</p>	<p>We have inspected the procedure for the prevention of data leakage.</p> <p>We have inspected documentation showing that technological measures for the prevention of data leakage have been implemented.</p>	No deviations noted.

## A.8 Technological controls

Control objective: To ensure the continuous operation of information processing facilities, including the recovery from loss of data or systems.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.13	<p><i>Information backup</i></p> <p>Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.</p>	<p>We have inspected the procedure for backup.</p> <p>We have inspected that the backup procedure is updated and approved.</p> <p>We have, by sample test, inspected documentation showing that backups are carried out in accordance with the procedure, including reports and system extracts with the status of backup jobs.</p> <p>We have, by sample test, inspected documentation for completed restore tests, including that backup data has been successfully restored, and that the most recent test was carried out within the audit period.</p>	No deviations noted.
8.14	<p><i>Redundancy of information processing facilities</i></p> <p>Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.</p>	<p>We have inspected that documented requirements for redundancy in system architecture and IT landscape exist, including an alternative location for the storage of data and backups.</p> <p>We have inspected documentation for implemented controls that support redundancy in components and processing activities.</p> <p>We have inspected documentation for implemented redundancy measures.</p>	No deviations noted.

## A. Technological controls

Control objective: To record events, generate evidence, ensure the integrity of log information, prevent against unauthorised access, detect anomalous behaviour and identify information security events and incidents.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.16	<p><i>Monitoring activities</i></p> <p>Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.</p>	<p>We have inspected the procedure for monitoring activities.</p> <p>We have inspected documentation showing that monitoring has been implemented.</p>	No deviations noted.
8.17	<p><i>Clock synchronisation</i></p> <p>The clocks of information processing systems used by the organisation should be synchronised to approved time sources.</p>	<p>We have inspected that clocks used by the organisation for information processing and supporting information processing systems are synchronised with approved time sources.</p>	No deviations noted.

## A. Technological controls

Control objective: To ensure the integrity of operational systems and application controls as well as to prevent exploitation of technical vulnerabilities.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.18	<p><i>Use of privileged utility programs</i></p> <p>The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.</p>	<p>We have inspected the procedure for access to privileged supporting programs.</p> <p>We have inspected that access to privileged supporting programs is technically restricted and that procedures have been established.</p> <p>We have inspected that requirements for logging changes and attempts to use supporting programs have been defined, and that extraordinary actions are logged.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.19	<p><i>Installation of software on operational systems</i></p> <p>Procedures and measures should be implemented to securely manage software installation on operational systems.</p>	<p>We have inspected the procedure for software installations on operating systems.</p> <p>We have inspected documentation showing that a system for the deployment of patches has been set up, as well as alerting in connection with failed patches.</p>	No deviations noted.

## A. Technological controls

Control objective: To ensure the protection of information in networks and its supporting information processing facilities.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.20	<p><i>Networks security</i></p> <p>Networks and network devices should be secured, managed and controlled to protect information in systems and applications.</p>	<p>We have inspected the policy for networks and network devices.</p> <p>We have inspected documentation showing that implementation and specific security measures are documented through technical configurations.</p>	No deviations noted.
8.22	<p><i>Segregation of networks</i></p> <p>Groups of information services, users and information systems should be segregated in the organisation's networks.</p>	<p>We have inspected the network security policy.</p> <p>We have inspected that the network is segmented into several zones, including DMZ, guest network, and internal networks.</p>	No deviations noted.
8.23	<p><i>Web filtering</i></p> <p>Access to external websites should be managed to reduce exposure to malicious content.</p>	<p>We have inspected that web filtering mechanisms have been established and that technical restrictions prevent access to prohibited websites.</p> <p>We have inspected that an updated list of blocked external websites exists.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.24	<p><i>Use of cryptography</i></p> <p>Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.</p>	<p>We have inspected the policy for the use of cryptography.</p> <p>We have inspected that information is protected in accordance with the cryptography policy, and that configuration reports as well as compliance reports confirm adherence to the policy.</p> <p>We have inspected VPN configurations, which document the use of strong encryption algorithms to protect data traffic.</p>	No deviations noted.

## A.8 Technological controls

Control objective: To ensure information security is designed and implemented within the secure development life cycle of software and systems.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.25	<p><i>Secure development life cycle</i></p> <p>Rules for the secure development of software and systems should be established and applied.</p>	<p>We have inspected the procedure for secure development.</p> <p>We have inspected that the procedure has been updated and approved by management during the audit period.</p>	No deviations noted.
8.26	<p><i>Application security requirements</i></p> <p>Information security requirements should be identified, specified and approved when developing or acquiring applications.</p>	<p>We have inspected the procedure for secure development.</p> <p>We have inquired whether there have been development projects during the audit period.</p>	<p>We have been informed that there have not been any development projects during the audit period.</p> <p>No deviations noted.</p>
8.27	<p><i>Secure system architecture and engineering principles</i></p> <p>Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.</p>	<p>We have inspected the principles for the development of information systems.</p> <p>We have inspected that the principles for the development of information systems have been approved.</p> <p>We have inspected that the principles are updated and maintained.</p>	No deviations noted.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.28	<p><i>Secure coding</i></p> <p>Secure coding principles should be applied to software development.</p>	<p>We have inspected the procedure for software development.</p> <p>We have inquired whether there have been development projects during the audit period.</p>	<p>We have been informed that there have not been any development projects during the audit period.</p> <p>No deviations noted.</p>

## A.8 Technological controls

Control objective: To validate if information security requirements are met when applications or if codes are deployed to the production environment.

No.	IT Forum Gruppen A/S' control	Grant Thornton's test	Test results
8.29	<p><i>Security testing in development and acceptance</i></p> <p>Security testing processes should be defined and implemented in the development life cycle.</p>	<p>We have inspected procedures for security testing in the development lifecycle.</p> <p>We have inspected documentation showing that automatic and manual security tests are defined and implemented.</p> <p>We have inquired whether there have been development projects during the audit period.</p>	<p>We have been informed that there have not been any development projects during the audit period.</p> <p>No deviations noted.</p>
8.31	<p><i>Separation of development, test and production environments</i></p> <p>Development, testing and production environments should be separated and secured.</p>	<p>We have inspected the procedure for the separation of development, test, and production environments.</p> <p>We have inspected that separation of duties has been established among employees with access to development, test, and production environments.</p>	<p>No deviations noted.</p>
8.32	<p><i>Change management</i></p> <p>Changes to information processing facilities and information systems should be subject to change management procedures.</p>	<p>We have inspected the procedure for change management.</p> <p>We have, by sample test, inspected that changes to systems have been implemented according to the procedure, including that they have been planned, approved, and tested.</p>	<p>No deviations noted.</p>