EG Danmark A/S and EG Norge AS

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2025 to 31 December 2025 in relation to EG Danmark A/S and EG Norge AS's development and operating services regarding EG Healthcare

July 2026

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Contents

1. Management's assertion 3
2. Independent service auditor's assurance report on the description, design and operating effectiveness of controls 5
3. Description of services and relevant controls 8
4. Control objectives, control activity, tests and test results 16

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

1. Management's assertion

The accompanying description has been prepared by EG Danmark A/S and EG Norge AS (EG) for customers who have used EG's development and operating services regarding EG Healthcare and their auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements in their financial statements.

Microsoft Ireland Operations Ltd and team.blue Denmark A/S are service organisations that provide hosting and backup services to EG. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of EG and excludes the control objectives and related controls of Microsoft Ireland Operations Ltd and team.blue Denmark A/S. Our evaluation did not extend to controls of Microsoft Ireland Operations Ltd and team.blue Denmark A/S.

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

EG confirms that:

a) The accompanying description in section 3 fairly presents IT general controls in relation to EG's development and operating services regarding EG Healthcare that have processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to EG's development and operating services regarding EG Healthcare were designed and implemented, including:

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

   (ii) Includes relevant details of changes to IT general controls in relation to EG's development and operating services regarding EG Healthcare during the period from 1 January 2025 to 31 December 2025

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

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.

Aarhus, 2 July 2026
EG Danmark A/S and EG Norge AS

Laila Aarseth
Vice President

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2025 to 31 December 2025 in relation to EG's development and operating services regarding EG Healthcare to customers

To: EG Danmark A/S and EG Norge AS (EG), their customers and their auditors

Scope

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

Microsoft Ireland Operations Ltd and team.blue Denmark A/S are service organisations that provide hosting and backup services to EG. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of EG and excludes the control objectives and related controls of Microsoft Ireland Operations Ltd and team.blue Denmark A/S. Our examination did not extend to controls of Microsoft Ireland Operations Ltd and team.blue Denmark A/S.

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

EG's responsibilities

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

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

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

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

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

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

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

Inherent limitations

EG's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of EG's development and operating services regarding EG Healthcare that the individual customer may consider important in its own particular circumstances. Also, because of their nature, controls at a service organisation or subservice organisation may not prevent or detect all errors or omissions in EG's development and operating services regarding EG Healthcare. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

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

a) The description fairly presents how IT general controls in relation to EG's development and operating services regarding EG Healthcare were designed and implemented throughout the period from 1 January 2025 to 31 December 2025

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

c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

Description of test of controls

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

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Intended users and purpose

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

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

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

Aarhus, 2 July 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

3. Description of services and relevant controls

3.1. Description of services covered by the report

The services offered by EG and covered by this report are the following:

- Providing applications in Software-as-a-Service model
- Providing applications in a Managed Service model in which the applications and the underlying infrastructure are managed by EG
- Providing applications (sale of licences) that subsequently are hosted and managed by EG's customers.

In order to ensure an adequate level of security irrespective of the model in which a particular application is provided, EG applies a common framework of controls described further in this document, focusing on application development as well as maintenance of applications and underlying infrastructure. As part of this framework, EG is responsible for ensuring the implementation and operation of control systems to prevent and detect errors, including intentional errors, in order to comply with contracts and best practice.

EG uses Microsoft Ireland Operations Ltd and team.blue Denmark A/S as subservice suppliers significant to the description and understanding of the scope of this report. Microsoft Azure and team.blue Denmark A/S provide hosting services, including data centre, hardware, storage and backup (up to the level of virtualisation platform). Microsoft Ireland Operations Ltd and team.blue Denmark A/S provide additional backup solutions and off-site storage. The controls applied by these service providers are not subject of this report. EG is strictly monitoring the level of security ensured by these providers and for 2025 obtained the audit reports from these suppliers.

3.2. Description of control environment

3.2.1. Information security policy (control objective A)

EG has drawn up an overall cyber and information security policy ("the IT security policy") based on security standards such as ISO 27001 and CIS Controls version 8.

The overall security framework at EG consists of:

- The cyber and information security policy
- Group-level policies, procedures and guidelines that apply to all EG companies
- Local security procedures and instructions in the individual business units or at EG companies.

EG Cyber and Information Security performs an annual review of the IT security policy as well as of the associated procedures and guidelines – including that these meet the external obligations set out by law and contracts/agreements.

The policies and activities of the Cyber and Information Security Management system introduce the set of "non-negotiable" security controls which must be implemented in every product and system operated in EG. Any exceptions from these controls are registered as formal risks and monitored:

- Endpoint Detection & Response (EDR) solution with Managed Detection & Response (MDR) service must be deployed on all EG endpoints.
- External vulnerability scans must be conducted on all internet-facing systems.
- Internal vulnerability scans must be performed regularly on all internal IT infrastructure.
- Multi-factor authentication (MFA) must be used everywhere for all accesses to our systems.
- Secure and tested backups must be maintained for all critical data and systems.
- Cloud environments must follow approved security baselines and be continuously monitored.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

3.2.2. Organisation of information security (control objective B)

The overall responsibility for IT security at EG and associated companies lies with the IT security committee (EG Security Committee) which deals with all major relevant IT security matters of a fundamental nature.

The IT security committee is represented by employees from top management, division managers, the vice president of IT, CIO, CISO and the general counsel of Group Legal & Compliance. The IT security committee reports directly to the Executive Board of EG. The committee is normative and, based on the adopted IT security policy, it lays down the principles and guidelines that are to ensure objectives are met. Security incidents, status and security weaknesses are reported to the IT security committee which initiates any further action. Like all other employees, members of the IT security committee regularly participate in relevant awareness training within IT security. The IT security is executed through internal strategy, policies, standards, procedures and guidelines.

The operational responsibility for the management of the cyber and information security in EG is placed on the central Cyber and Information Security Team headed by the chief information security officer (CISO). This team defines security policies, requirements and guidance for the whole EG organisation, coordinates implementation of security measures across the organisation and operates centrally delivered security processes. The Cyber and Information Security Team is responsible for ensuring that EG employees are kept up to date with the security regulations.

Particular responsibility for following security policies, requirements and guidance and implementation of required security measures lies on the organisational units that develop and maintain EG systems: EG IT, CloudOps, DevOps and individual business units. Those units nominate security coordinators who act as liaison to the Cyber and Information Security Team and who coordinate security activities in their units. They also nominate local security incident coordinators responsible for security incident management in these units.

All EG personnel, including employees and third parties with access to EG systems, have a responsibility to protect EG's information against unauthorised access, alteration, destruction and theft. Therefore, all employees are made familiar with the Security Handbook and are required to complete the required security trainings or assignments. Depending on the role in the organisation, employees are also communicated about specific security policies and procedures.

EG has established and maintains a Cyber and Information Security Management System (C&ISMS) with a goal to ensure an adequately high level of security, compliant with relevant legal and other external requirements. The C&ISMS takes a risk-based approach in ensuring the adequate security level. Security objectives, security strategy and decisions as to which security measures to apply take into account the impact and probability of risks addressed. Performance and effectiveness of the C&ISMS is monitored and evaluated, including effectiveness of key processes, status of actions to achieve security objectives or risk treatment plans, effectiveness of security measures, as well as risk and security levels. A combination of measures may be applied such as KPI measurement, audits, penetrations tests, security scans, risk assessments and management reviews. All identified nonconformities, weaknesses and improvement possibilities result in preparation of actionable plans to continually improve the suitability, adequacy and effectiveness of the C&ISMS.

Human resources security

The HR function is handled by HR at EG Denmark A/S and by the individual managers of the employees. The employees' security responsibilities are determined through an adequate job description and by the terms of the employment contract. Some employees are security cleared if this requirement has been agreed with the customer.

The employees receive education, training and information on information security through IT security awareness training to ensure an appropriate and relevant level that matches the employees' tasks, area of responsibility and capabilities. This also includes current information on known threats as well as information on who to contact for further advice on information security.

Upon appointment, employees sign an employment contract in which they undertake to comply with the company's IT security policy and continuously keep up to date with any changes. All guidelines and policies are available to the employees on EG's intranet. EG informs the employees in writing on EG's intranet in case of updates/changes to the IT security policy.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

The individual employee is responsible for complying with the IT security policy, the Security Handbook and the rules that are relevant to the employee's tasks. The employee is also responsible for reporting any breaches of IT security or suspicion thereof to the IT security function. EG has internal procedures for handling employee violations of EG's security rules and procedures.

Security incident management

All security incidents are handled according to the established Security Incident Management Policy and procedures. If an employee becomes aware of a security incident, he or she must inform the appointed security incident manager, who is responsible for ensuring a quick, effective and timely response to information security incidents.

In the event of a security incident, the affected customers are notified as soon as possible, and steps are taken to secure data and systems. If agreed with the customer, a root cause analysis report is drawn up to ensure, as far as possible, that the incident cannot occur again.

All material security incidents are reported to Management.

External parties and supplier relationships

EG has formal procedures for entering into agreements and contracts with suppliers and consultants. These procedures ensure that the supplier meets the security obligations and requirements to which EG is subject through contracts and legislation. All new suppliers must be approved by the Vendor Approval Board, which assesses the supplier's ability to meet applicable security and compliance requirements.

Agreements are maintained through close dialogue and regular meetings with our suppliers. Supplier agreements are regularly optimised in respect of our situation and our customers.

3.2.3. Physical security (control objective C)

Secure physical boundaries are established to protect areas with information processing equipment and storage media.

Securing of offices, rooms and facilities

All of EG's buildings are secured according to a recognised standard in a very high safety class used in places where highly valuable assets or sensitive personal/customer data are handled.

Alarm systems as well as access control systems are subject to monitoring 24-7 by EG Facility and the guard's control centre.

Access to the company's premises is controlled by access cards. Access rights are aligned with the information recorded by HR. If an employee or a supplier loses his/her access card, access will be blocked as soon as it comes to our attention or as soon as abuse is identified.

Visitors who need access to the building must be under constant monitoring by the host. Visitors to the building and the time of their visit are logged.

Data centres

Data centres are operated by third parties. Through contracts and agreements, EG has ensured that the data centre protection meets the ISO 27001 standard, including that data centres are protected against internal and external threats (environmental disasters and power outages) and that the security is regularly maintained and tested. Access to server rooms can only be granted to individuals with authorised access approved by the hosting provider or by EG.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

3.2.4. Communications and operations management (control objective D)

Operating procedures

Procedures are in place to ensure that the availability of systems and data can be maintained and that operations can continue in the event of disruptions. This is ensured through preventive, detective and corrective controls, among other things. The controls are physical controls, procedural controls, technical controls and statutory controls. These controls e.g. cover authentication, antivirus, firewall, incident management, monitoring, backup and contingency plans.

The operating system is patched continuously.

The customer's data is secured by building the network structure by VLANs so that each customer can only access its own network.

Formal change management procedures have been prepared in order to minimise the risk of compromising company and customer information. The introduction of new systems and major changes to existing systems follow a formal process of documentation, specification and controlled implementation.

Monitoring and logging

Effective monitoring of processes provides important information for both proactively and reactively being able to avoid events that would otherwise affect security or compliance with the guaranteed availability of systems. The aim is to minimise the time it takes to restore normal operations. Additionally, a key security objective is to promptly identify and respond to security threats or incidents through continuous monitoring, ensuring the integrity and availability of systems and data are maintained.

To accommodate this, the company works with preventive monitoring and related corrective actions. With this method, there is no or minimal impact on security and compliance with the availability of the systems agreed with customers.

Where it is not possible to predict events, detective monitoring with associated corrective actions is used.

EG uses endpoint detection and response tools on every server and workstation as well as cloud protection tools in order to continuously monitor for any suspicious activity and block attacks in real time. External managed detection and response service providers monitor EG endpoints and cloud workloads continuously 24/7, respond to alerts and escalate issues to relevant teams.

EG uses an event management tool to handle automatic monitoring of servers, system software and application software. The monitoring typically covers RAM, disk space, CPU consumption or whether specific applications are running. Monitoring and notification are set as agreed for the application.

EG uses a security information management system that allows for logging. Log consolidation and secure storage of documentation through a single console allow you to access and manage all information. The archive will ensure that no log messages are lost in the event of a system crash or a hacker attack.

Our communication to customers in respect of security of operations and data takes place according to the procedures agreed with the individual customer under the contract.

In the event of a security incident, the affected customers will be contacted as soon as possible.

Segregation of duties

Policies and procedures are established to ensure segregation of duties. Among other things, they include requirements that the responsibilities for development and for updates to the production environment are segregated and that development and operational activities are segregated.

If segregation of duties is not practically or financially appropriate, it must be possible for the employees to break with this principle. This e.g. applies to developers who can make changes directly in the operating environments if necessary.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Backup data is stored separately from production data in accordance with the principles of segregation of duties and isolated at both the network and identity layers.

Encryption

A policy and a set of procedures have been developed to ensure relevant and necessary encryption of data.

As a general rule, encryption is used on external communication to and from the company and to and from data centres. Either IPsec VPN or SSL/TLS is used.

Encryption at rest is applied on filesystem or database level where this was requested and agreed with the customers.

Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.

TLS encryption in connection with the transmission of emails complies with applicable requirements in the area.

Backup and restore

EG ensures that backup and restore comply with applicable EG standards and are in accordance with the agreement with the customer. The detailed principles and procedures for backup and restore are stated in the individual agreement with the customer.

Backups are set up to meet recovery point and recovery time objectives. Backups are encrypted, protected from tampering through immutability or isolation, and regularly tested to confirm they can be restored within the required recovery time objective.

Error correction and support

EG applies the principles of ITIL (IT Infrastructure Library). ITIL is a collection of best practices based on experience from private and public companies. ITIL defines a number of IT processes within IT service management, and ITIL has a process-oriented approach to the IT organisation. Many support systems focus their efforts on establishing digital workflows that support ITIL processes. For this purpose, EG works with an ITSM support system supporting this workflow. The support system is continuously developed with associated forums for teaching new functionality. In addition, several executives and operational employees are ITIL-certified.

Incident management is anchored in EG's support system which can be contacted through the associated customer portal, by email or through the call centre. In the support system, all incidents are registered and prioritised in accordance with applicable guidelines.

Reporting to customers takes place if required in the agreement with the customer.

3.2.5. Access management (control objective E)

In order to manage access to the company's systems, information and networks, rules have been established for granting, changing and revoking access and rights to all EG systems.

Access management has been implemented for the handling and approval of both internal and external user accesses.

Employee access to company systems takes place using multi-factor authentication (MFA) wherever technically feasible. Access to systems is limited to employees with a work-related need based on the principle of roles and rights management. The technical administration of authorisations for EG's internal systems and data is managed by EG IT.

User rights are periodically reviewed, and all access must be approved by the immediate manager to ensure that only people with a work-related need have access to systems. The procedure ensures that users no longer having a work-related requirement for access will be deleted during the review.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

All employees and external users' access are revoked when the employment terminates.

3.2.6. Acquisition, development and maintenance of operating systems (control objective F)

EG is responsible for vulnerability and patch management on systems in the data centres. The purpose is to ensure that vulnerabilities in the systems are timely identified and remediated, and patches are timely applied. This applies to systems used internally as well as systems used by external customers (customer systems).

External vulnerability scans on all internet-facing systems and internal vulnerability scans on all internal IT infrastructure are performed regularly. Applications, operating systems, databases and third-party software are patched in accordance with the Vulnerability & Patch Management Policy and the recommendations of the respective suppliers. In addition, applications, operating systems, databases and third-party software are updated or replaced if they are no longer supported by the supplier.

Network devices are patched in accordance with the Vulnerability & Patch Management Policy and the recommendations of the network manufacturer. Similarly, network devices will be updated or replaced if firmware or hardware is no longer supported by the network manufacturer.

Standard patching:

In case of exceptions to the standard patch level, the selected patch level will be described. As a general rule, standard patching is provided.

It is a requirement that the supplier can select a service window for patching.

It is a requirement that patch management can be carried out with automatic restart of system/servers.

Exceptions that require special handling:

If systems cannot be patched automatically, and assistance from system consultants is needed each time patching is carried out, this must be clearly stated in the agreement.

- All security updates: For security reasons, these are installed as soon as possible.
- All update rollups for the operating system: It is recommended that these updates are installed after they have been evaluated and tested.
- All service packs for the operating system: They generally contain comprehensive changes and improvements to the systems and must be thoroughly tested in the environment before they are installed.

Process for approval of service packs

All service packs are assessed continuously in cooperation with the relevant people who have knowledge of the environment in question. If possible, service packs are tested in a pre-production environment before being installed in the production environment.

All patch routines are handled via a request for change in which any risks of installing the updates in question are assessed. This also includes an assessment of a fall-back plan as well as of how to handle any errors.

Change management

Changes to the organisation, processes, facilities and systems that affect information security are managed through a formal process. This implies that changes to operating systems and networks are tested by qualified personnel prior to being moved to production.

Tests of changes to operating systems and networks are approved before being moved to production.

Emergency changes to operating systems and networks that bypass the normal business process are tested and approved subsequently.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

3.2.7. Acquisition, development and maintenance of applications (control objective F)

Development takes place according to state-of-the-art agile principles; through user involvement and engagement, we make sure that our solutions meet our customers' requirements.

Security, usability and stability are the cornerstones and foundation of all products developed by EG. The Software Development Life Cycle (SDLC) Policy defines minimum requirements for the life cycle of EG products.

Security controls are implemented into the software development lifecycle. All code and software components used in EG's applications are tested or scanned with security software to identify and fix vulnerabilities.

When it comes to larger-scale and more basic features, the following process takes place:

- Market validation through involvement of customers according to needs and requirements, if relevant
- Prototype development and relevant involvement of customers in this process
- Development and continuous release to all or specific customers
- Monitoring of use and, if relevant, adjustment
- Release of feature to all or specific customers
- Training of users through a well-designed interface and related articles on the support site
- Subsequent user support by phone or by email to the support system
- Continuous monitoring of use and any adjustments.

Other tasks, minor corrections, updates and error corrections are carried out continuously while taking scope, prioritisation and overall strategic focus into consideration.

Tasks, projects and planning are handled in the task management system. The task management system is directly linked to source code changes, allowing for full traceability of new features and error corrections.

3.2.8. Disaster recovery plan (control objective G)

EG has drawn up a set of crisis management and disaster recovery plans with the aim of ensuring that EG can keep critical business processes running in the event of a disaster.

EG has drawn up disaster recovery plans which describe the disaster organisation, i.e. descriptions of Management roles, contact information, notification lists and instructions for the requisite disaster task forces.

The disaster recovery plans for EG include:

- Measures to mitigate damage
- Establishment of temporary emergency solutions
- Re-establishment of a permanent solution.

The disaster recovery plans are updated and tested once a year to ensure that they are adequate and effective.

3.3. Complementary controls at the customers

Assumptions regarding customer responsibility are described in the individual contracts. Customers are responsible for their own data. This means that customers are responsible for any data changes made when individual usernames and passwords are used to log into the system. In case of third-party access requested by a customer, the customer is responsible for following up on the control.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

3.4. Improvements

In 2025, EG has taken the following measures to improve the level of security and data protection:

Month	Measures

November 2025	**In 2025, EG strengthened its position in cyber security and data protection through a range of strategic and operational initiatives.**
	
	• Our governance structure was reinforced through our cyber and information security framework, ensuring alignment with applicable requirements such as the CIS Controls, NIS2, the AI Act and GDPR.
	
	• We implemented key technical and organisational improvements, including:
	  ○ Expanded application security testing and enhanced vulnerability management capabilities
	  ○ Improved cloud security governance
	  ○ Expanded asset management through integrations with a central CMDB
	  ○ Further strengthened third-party risk management through new classification and assessment criteria as well as internal tools.
	
	Infrastructure and application security were enhanced through stricter data protection and security standards, automated vulnerability scanning, and an expanded penetration testing programme for applications and infrastructure.
	
	Data protection measures were updated and strengthened through comprehensive data classification, encryption standards, and updated testing of incident reporting processes to support new legislation such as NIS2.
	
	EG further invested in awareness training to raise employee security awareness and in continuous compliance monitoring to embed a culture of resilience and regulatory readiness across the organisation.
	
	EG implemented and rolled out guidelines for generative and agentic AI and MCP server governance, including approval workflows and integration patterns. EG has:
	
	• established formal working procedures to define and govern the secure adoption of AI across products and internal processes
	
	• introduced AI-assisted tools that connect vulnerability data to developers' workflows, and launched an AI-based threat modelling tool to accelerate consistent documentation and risk assessments
	
	Finally, EG revised the system descriptions in the audit statements to reflect new applicable legislation and to incorporate the relevant organisational changes resulting from these legal updates.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

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

4.1. Purpose and scope

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

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

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

4.2. Test actions

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

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

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

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

Control objective A: Information security policy

Management has prepared an information security policy which outlines clear IT security objectives, including choice of framework and resource allocation. The information security policy is maintained with due consideration of an up-to-date risk assessment.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
A.1	**Written information security policy** Management has documented a set of policies for information security which are reviewed and maintained at least once a year and in the event of significant changes. The policy has been approved by Management. The security policy has been made available to employees and relevant external parties through the shared documentation. The security policy contains requirements for maintaining relevant segregation of duties to reduce the risk of unauthorised access, use or abuse of rights. HR is responsible for carrying out personal as well as professional background verification checks on job candidates in accordance with relevant laws, regulations and ethical rules.	We made inquiries of Management about the procedures/control activities carried out. We inspected that Management has approved the security policy and that the policy is subject to review at least once a year. We also inspected that the policy is easily accessible to the employees.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective B: Organisation of information security

The organisational responsibility for information security is appropriately documented and implemented, and security is given high priority in agreements with external parties.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
B.1	**Management's information security responsibilities** The organisational information security responsibilities, including responsibilities and roles, are defined in the security policy. Moreover, rules have been laid down in relation to non-disclosure agreements and reporting on information security incidents, and a record of assets has been prepared. The appointed security incident managers in the business unit and in the group are responsible for ensuring a quick, effective and orderly response to information security incidents. Information security incidents must be reported, and the security incident manager must be contacted as quickly as possible. Users who experience software errors report this to Service Desk. According to the security policy, all reported information security incidents must be classified.	We discussed information security management in general terms with Management. We inspected that the organisational responsibility for information security has been documented and implemented. By inspection, we furthermore checked that non-disclosure agreements, reporting on information security incidents and records of assets have been prepared.	No exceptions noted.
B.2	**External parties** Risks related to external parties are identified, and security in third-party agreements as well as security issues related to customers are addressed. In the event of changes that affect the operating environment and where services from an external third party are used, these are selected and approved by Management. Only recognised suppliers are used.	We made inquiries of Management about the procedures/control activities carried out. We inspected that adequate procedures for collaboration with external suppliers have been established. Through random sampling, we also inspected that cooperation with external parties is based on approved contracts.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective C: Physical security

Operations are conducted out of premises protected from damage resulting from physical factors such as fire, water leaks, power outage, theft or vandalism.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
C.1	**Physical security perimeter** Access to secure areas that contain either sensitive or critical information (for both new and existing employees) is physically secured by restricting access to authorised employees through access cards. This requires documented Management approval. Individuals without clearance to access secure areas must be registered and accompanied by an employee with the appropriate authorisation.	We made inquiries of Management about the procedures/control activities carried out. During our visit to the data centres, we observed that access to secure areas is restricted by use of an access system. Through a random inspection, we reviewed procedures for physical security in secure areas to assess whether access to these areas is subject to documented Management approval and whether individuals without authorisation are registered and accompanied by an employee with proper authorisation. Through a random inspection, we moreover inspected employees with access to secure areas and inspected that documented Management approval has been granted.	No exceptions noted.
C.2	**Securing offices, rooms and facilities** All of EG's buildings are secured with alarm systems and monitored 24-7. Everyone who moves around EG's buildings must carry a visible ID card. All visitors are registered by the receptions on arrival. Consultants who need access to secure areas sign an NDA. Access rights are aligned with the information recorded by HR. If an employee or a supplier loses their access card, access will be blocked as soon as it comes to our attention or as soon as abuse is identified. The areas of the buildings are divided into the following sections:	We made inquiries of Management about the procedures performed. We inspected all server rooms and verified that access routes have been secured by use of a card reader. Through random sampling, we inspected that periodic reviews are performed.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective C: Physical security

Operations are conducted out of premises protected from damage resulting from physical factors such as fire, water leaks, power outage, theft or vandalism.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
	1) Public areas: Here, everyone can move around after registration. Both visitors, employees and suppliers have access. 2) Production and development areas: In all production areas, a valid access card is required, and access can only be gained through the access control system. Outside opening hours, a PIN code is moreover required. 3) Particularly secure areas (e.g. server rooms, rooms where particularly sensitive data is handled): Access to these areas always requires access card and use of a PIN code. A policy has been drawn up specifying that desks are to be kept clear of paper and removable storage media and that screens of information processing facilities must be blank.		
C.3	**Siting and protection of equipment** Data centres are protected from environmental disasters such as fire, water and heat. Data centres are located a safe distance from other buildings and placed above water and ground level. Redundant cooling units are used, and data centres are fire protected with a "sniffer" system that notifies and activates the Inergen system. Data centres are equipped with cameras, IR sensors and alarms inside and outside, and areas are completely fenced. Only operations technicians have access to data centres, and all visits are recorded via access cards and video surveillance.	We made inquiries of Management about the procedures/control activities carried out. By inspection, we reviewed the operating facilities and inspected that firefighting systems, monitoring of indoor climate and cooling in the data centres are in place. Through a random inspection, we reviewed documentation of equipment maintenance to confirm that such maintenance is performed on an ongoing basis.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective C: Physical security

Operations are conducted out of premises protected from damage resulting from physical factors such as fire, water leaks, power outage, theft or vandalism.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
	Data centres are operated by third parties.		
C.4	**Supporting utilities (security of supply)** Data centres are connected to two separate electric power connections – a local generator station and a diesel generator that take over in the event of power failure on the grid. Data centres are operated by third parties.	We made inquiries of Management about the procedures/control activities carried out. During our visits to the data centres, we observed that monitoring of UPS or emergency power facilities takes place. Through a random inspection, we reviewed documentation of equipment maintenance to confirm that UPS or emergency power facilities are maintained and tested on an ongoing basis.	No exceptions noted.
C.5	**Securing of cables** All network cables are located in server rooms, thus reducing the risk of environmental threats and the risk of unauthorised access. Data communication and electricity cables are protected from unauthorised interference and damage. Data centres are operated by third parties.	During our inspection, we observed that cables for the supply of electricity and data communication are protected against damage and unauthorised actions.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective D:

The below measures have been established:

- Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents
- Sufficient procedures for backup and contingency plans
- Appropriate segregation of duties in relation to IT functions, including between development, operations and user functions
- Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
D.1	**Documented operating procedures** Management has implemented operating routines and an associated process for execution and follow-up on operations. The operating procedures are documented and made available to anyone who needs them.	We made inquiries of Management about whether all relevant operating procedures are documented. In connection with the audit of each area of operation, we checked by inspection that documented procedures are in place and that there is consistency between documentation and actions performed. By inspection, we also verified that adequate monitoring and follow-up on this are performed.	No exceptions noted.
D.2	**Segregation of duties** Management has implemented policies and procedures to ensure satisfactory segregation of duties in the IT department. These policies and procedures include the following requirements: • The responsibility for development and updates to the production environment are to be segregated. • The IT department does not have access to applications and transactions. • Development and operating activities are segregated. Segregation of duties is the fundamental control principle at personal as well as organisational level. If segregation of duties is not practically or financially appropriate, it must be possible for the	We made inquiries of Management about the procedures/control activities carried out. We inspected users with administrative access rights to verify that access is based on a work-related need and does not compromise segregation of duties in relation to the development and production environments.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective D:

The below measures have been established:

- Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents
- Sufficient procedures for backup and contingency plans
- Appropriate segregation of duties in relation to IT functions, including between development, operations and user functions
- Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
	employees to break with this principle. This e.g. applies to developers who can make changes directly in the operating environments if necessary. Thus, a reservation for segregation of duties is made in certain cases. However, segregation of duties applies to critical systems. Backup data is stored separately from production data in accordance with the principles of segregation of duties.		
D.3	**Measures to protect against viruses and similar malicious code** Controls have been established to protect against malware and similar malicious code. It is ensured that antivirus is installed and updated regularly on all computers.	We made inquiries of Management about the procedures/control activities carried out. Through a random inspection, we reviewed the technical set-up to confirm that antivirus programs are installed and that they are up to date.	No exceptions noted.
D.4	**Information backup** Backup copies of customer data are made continuously. Daily reports are received from the backup system specifying whether the backup has been successfully completed. If this is not the case, the issue is escalated to the person responsible. Backup of data is made, and regular tests are performed to verify that data can be restored from backup files.	We made inquiries of Management about the procedures/control activities carried out, reviewed the backup procedures and verified that they are adequate and formally documented. Through a random inspection, we reviewed backup logs to confirm that backup has been successfully completed, alternatively that remedial measures have been taken in case of backup failure. We reviewed the restore log by a random inspection.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective D:

The below measures have been established:

- Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents
- Sufficient procedures for backup and contingency plans
- Appropriate segregation of duties in relation to IT functions, including between development, operations and user functions
- Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
		We inspected the procedure for external storage of backup tapes to confirm that backups are stored safely.	
D.5	**Monitoring of system use and audit logging** Logging of access to critical systems has been implemented. These logs will be reviewed in case of suspicion of abuse or errors. Security incident managers follow up on security incidents and ensure that access to system components is logged. According to the security policy, logging facilities and log information are protected against tampering and technical errors. **Administrator and operator logs** High-risk operating systems and network transactions or activity as well as users with privileged rights are subject to monitoring. Any deviations are examined and resolved in a timely manner.	We made inquiries of Management about the procedures/control activities carried out and reviewed the system set-up on servers and important network units. Furthermore, we inspected that logging parameters are set up to ensure that actions performed by users with extended access rights are logged. Through a random inspection, we furthermore checked that adequate follow-up on logs from critical systems is performed.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective D:

The below measures have been established:

- Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents
- Sufficient procedures for backup and contingency plans
- Appropriate segregation of duties in relation to IT functions, including between development, operations and user functions
- Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
D.6	**Debugging** Management has established procedures for support management. These include a preliminary assessment of whether an incident may be classified as critical and thus is to be given high priority. The assessment is made on the basis of established guidelines which are accessible to everyone who handles support: Classification of incidents (prioritisation based on impact and urgency): • Match incidents with previously identified incidents, problems and known errors • Initiate relevant RFCs when the circumstances surrounding the incident have been clarified. Follow-up on incidents reported is performed continuously, and incidents are escalated, if considered necessary.	We made inquiries of Management about the procedures/control activities performed and reviewed the procedure for handling incidents. Through a random inspection, we inspected that incidents are classified, that there is a match between incidents and previously identified incidents and that relevant RFCs are initiated in a timely manner.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective E: Access management

The below measures have been established:

- Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data
- Logical and physical access controls reducing the risk of unauthorised access to systems or data
- Logical access controls supporting organisational segregation of duties.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
E.1	**User registration and privilege administration** An access control policy has been established which specifies that allocation and use of access rights to operating systems, networks, databases and data files for new and existing users are reviewed to ensure compliance with company policies. It is ensured that rights are granted on the basis of a work-related need and are approved and created correctly in the systems. The head of department approves user rights.	We made inquiries of Management about the procedures/control activities carried out. We inspected the procedures for user administration and checked that control activities are adequate. Through a random inspection, we checked that access to data and systems is granted based on a work-related need and has been approved in accordance with business processes.	No exceptions noted.
E.2	**Administration of user access codes (passwords)** Access to operating systems, networks, databases and data files is protected by use of passwords. To ensure quality passwords, requirements have been established for the quality of passwords, i.e. minimum length, complexity and expiry, and password settings ensure that passwords cannot be reused. Moreover, the user will be locked out after several failed login attempts. A tool is used for password management.	We made inquiries of Management about procedures/control activities carried out in connection with password controls, and we inspected that users are subject to appropriate authentication on all access points. By inspection, we checked that the password quality used in EG's operating environment is appropriate, and, by carrying out sample tests, we inspected that company systems are accessed on the basis of username and password.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective E: Access management

The below measures have been established:

- Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data
- Logical and physical access controls reducing the risk of unauthorised access to systems or data
- Logical access controls supporting organisational segregation of duties.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
E.3	**Assessment of user access rights** Periodic reviews of user rights are performed to ensure alignment with the users' work-related needs. These reviews ensure that users only have access to the networks and network services that they have been specifically authorised to use. Discrepancies are investigated and resolved in a timely manner to ensure that access is restricted to people who need it.	We made inquiries of Management about the procedures/control activities carried out. Through a random inspection, we checked that periodic reviews are carried out to confirm that these have taken place, and we inspected that identified deviations are subject to remedial action.	No exceptions noted.
E.4	**Revocation of access rights** A fixed procedure has been implemented which ensures that user rights granting access to operating systems, networks, databases and data files pertaining to terminated employees are revoked in a timely manner. The rights of access, including remote access, of employees and external users are removed upon termination of their employment, contract or agreement, or adjusted upon change.	We made inquiries of Management about the procedures/control activities carried out to ensure that access rights are revoked in accordance with adequate business processes and that the rights granted are followed up on in accordance with the business processes. Furthermore, through a random inspection, we checked that the business processes described are being complied with as regards deleted user accounts on systems and that inactive user accounts are disabled on termination of employment.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective E: Access management

The below measures have been established:

- Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data
- Logical and physical access controls reducing the risk of unauthorised access to systems or data
- Logical access controls supporting organisational segregation of duties.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
E.5	**Policy on use of network services, including authentication of users with external connections** To protect information in systems and applications, data communication is appropriately organised and adequately secured against the risk of loss of authenticity, integrity, availability and confidentiality. MFA or VPN is used when employees need external access to systems. Where necessary or agreed with the customer, networks are segregated. Access through external connections is granted through a formal administration process, and users who use an external connection are required to follow the organisation's practices. The security policy specifies that the use of secret authentication information must follow the organisation's practices.	We made inquiries of Management about the procedures/control activities carried out, and we inspected that an appropriate authentication process is applied to the operating environment. Through a random inspection, we checked that users are identified and verified prior to access being granted and that remote access is VPN-protected. By inspection, we ascertained that the network is segmented into smaller networks using VLANs and DMZs to reduce the risk of unauthorised access.	No exceptions noted.
E.6	**Management of network connections** Periodic penetration tests are carried out using a security scanner. Selected IP ranges are tested to check that firewall rules are set up correctly. The security policy specifies that EG IT has the overall responsibility for protecting the organisation's network. Employees may connect equipment to the network according to agreement with the IT department, and access to the network can	We made inquiries of Management about the procedures/control activities performed to manage network connections. By inspection, we ascertained that penetration tests have been carried out at regular intervals and that identified weaknesses have been assessed. Through a random inspection, we reviewed the firewall configuration and verified that firewall rules are set up appropriately.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective E: Access management

The below measures have been established:

- Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data
- Logical and physical access controls reducing the risk of unauthorised access to systems or data
- Logical access controls supporting organisational segregation of duties.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
	only take place through security-cleared solutions. Guests must use EG's guest network.		
E.7	**Limited access to information** Only people who need access to customer-specific systems have access. All access requests for new and existing users concerning applications, databases and data files are reviewed to ensure compliance with company policies; this ensures that rights are granted on the basis of a work-related need, are approved and are created correctly in systems. According to the security policy, access to systems is managed by a procedure for secure log-on. The security policy specifies formal policies and procedures for the transfer of protected information, including sensitive personal data, via electronic messaging. These policies and regulations deal with the secure transfer of sensitive information between the organisation and external parties.	We made inquiries of Management about the procedures/control activities carried out in order to limit access to information. We inspected the procedures for user administration and checked that control activities are adequate. Through a random inspection, we checked that access to data and systems is granted based on a work-related need and has been approved in accordance with business processes.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective F: Acquisition, development and maintenance of operating systems

Appropriate business processes and controls have been established for implementation and maintenance of operating systems.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
F.1	**Management of software on operational systems** Separate IT environments for development, testing and production have been established. Only functionally segregated employees are able to migrate changes between the individual environments. A procedure for managing the installation of software and changes to operational systems has been implemented. Follow-up on technical vulnerabilities of applied information systems is performed regularly, and the exposure to such vulnerabilities is assessed. In the event of changes to customer-specific systems, tests are performed where this has been agreed. Applications, operating systems, databases and third-party software are patched in accordance with the recommendations of the respective suppliers. In addition, applications, operating systems, databases and third-party software are updated or replaced if they are no longer supported by the supplier. Network devices are patched in accordance with the recommendations of the network manufacturer. Similarly, network devices will be updated or replaced if firmware or hardware is no longer supported by the network manufacturer.	We made inquiries of Management about the procedures/control activities carried out in order to maintain separation of the individual environments. By inspection, we verified that changes are tested in the test environment. Through a random inspection, we reviewed changes made during the period and inspected that the changes have been documented.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective F: Acquisition, development and maintenance of operating systems

Appropriate business processes and controls have been established for implementation and maintenance of operating systems.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
F.2	**Change management** Changes to the organisation, processes, facilities and systems that affect information security are managed through a formal process. This implies that changes to operating systems and networks are tested by qualified personnel prior to being moved to production. According to the security policy, security tests must be performed as required. Tests of changes to operating system and networks are approved before being moved to production. Emergency changes to operating systems and networks that bypass the normal business process are tested and approved subsequently.	We made inquiries of Management about the procedures/control activities performed, reviewed the adequacy of the change management procedures and verified that an appropriate change management system has been implemented and is supported by technical infrastructure. Furthermore, we inspected that a formal change management procedure has been implemented throughout the organisation. Through a random inspection, we reviewed change requests to check that: • Change requests are recorded in the established system. • Test of changes, including approval, are documented. • Approval must be obtained prior to implementation. Oral approval by Management is considered sufficient in connection with emergency changes but will have to be documented subsequently. • Where relevant, the plan for rollback is documented.	No exceptions noted.
F.3	**Change management / application development** EG uses formal procedures and tools to manage changes and development of applications. Change management and development are part of the release and deployment management procedures. No development is initiated unless there is a customer-defined or regulatory need for this.	We made inquiries of Management about the procedures/control activities performed and reviewed the adequacy of the change management procedures being part of the release and deployment management. We inspected that an appropriate change management system has been implemented and is supported by technical infrastructure.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective F: Acquisition, development and maintenance of operating systems

Appropriate business processes and controls have been established for implementation and maintenance of operating systems.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
	No changes to production are implemented before having been approved by an in-house developer and tested and before a fallback plan has been drawn up. Access to source code is limited to people with a work-related need. Only anonymous test data is used. In certain cases, it may be necessary to test on real data. In such cases, approval is obtained from the customer. Development, test and operating environments are segregated. All environments are subject to security requirements.		
F.4	**Release management applications** EG performs release management. A typical task solution process includes the following steps: • Specification of task in task management tool • Breakdown of task in cooperation with relevant persons (developer, product manager, etc.) • Development of functionality and continuous feedback • Development of automated testing • Code review by another developer • If relevant, adjustments in accordance with review • Preparation for deployment in test environment. For each release, the following is ensured: • Traceability with respect to each item of the release contents	We made inquiries of Management about the procedures/control activities performed and reviewed the adequacy of release management procedures. Through a random inspection, we checked whether traceability, coordination, management, sufficient and effective testing, code review, rollback plans and a process for communication to customers have been established before each release.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective F: Acquisition, development and maintenance of operating systems

Appropriate business processes and controls have been established for implementation and maintenance of operating systems.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
	• Coordination, involvement and management of the relevant parties in the context of a release • Coherent testing of the entire release, including integration testing and combined performance and load testing • Code review • Presence of roll-back plans for releases • Communication of new releases to customers.		
F.5	**Deployment management** For each release, procedures are in place to ensure that: • the test environment code is updated • automated tests of business rules are performed • automated tests of user interfaces are performed • manual regression tests are performed on an as-needed basis • code is prepared for updating and archiving following successful tests • all relevant environments are updated.	We made inquiries of Management about the procedures/control activities performed and reviewed the adequacy of deployment management procedures. Through a random inspection, we checked whether the code is updated and automatically tested based on business rules and user interfaces.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

Control objective G: Contingency plan

EG Danmark A/S is able to continue servicing its customers in case of a disaster situation.

No.	EG's control activity	Tests performed by PwC	Result of PwC's tests
G.1	**Structure of the contingency plan** The overall contingency plan consists of a high-level contingency procedure as well as operational contingency plans for the specific contingency areas which aim to ensure continuity in critical situations. The operational contingency plan includes a description of the contingency organisation, i.e. descriptions of Management roles, contact information, notification lists and instructions for the requisite disaster task forces. For the individual platforms, detailed task force instructions have been prepared concerning recovery and emergency operation in order to ensure information security continuity during adverse situations. The plan is revised once a year. **Test of the contingency plan** The contingency plan is revised and tested once a year to ensure its adequacy and effectiveness.	We made inquiries of Management about the procedures/control activities carried out. We inspected the materials provided on contingency, and we inspected that the organisational and operational IT contingency plan includes management function descriptions, contact information, notification lists as well as instructions.	No exceptions noted.

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Laila Aarseth
Kunde
On behalf of: EG Danmark A/S and EG Norge AS
Serial number: bankid.no no_bankid:9578-5994-4-461424
IP: 89.8.xxx.xxx
2026-07-02 10:24:17 UTC

QES

bankID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
On behalf of: PricewaterhouseCoopers Statsautoriseret…
Serial number: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-07-02 10:43:57 UTC

MitID

Penneo document key: IY5H5-CEFVF-7626O-8CSY1-4F5WM-R2RCG

This document is digitally signed using **Penneo.com**. The signed data are validated by the computed hash value of the original document. All cryptographic evidence is embedded within this PDF for future validation.

The document is sealed with a Qualified Electronic Seal. For more information about Penneo's Qualified Trust Services, visit **https://eutl.penneo.com**.

How to verify the integrity of this document
When you open the document in Adobe Reader, you should see that the document is certified by **Penneo A/S**. This proves that the contents of the document have not been modified since the time of signing. Evidence of the individual signers' digital signatures is attached to the document.

You can verify the cryptographic evidence using the Penneo validator, **https://penneo.com/validator**, or other signature validation tools.