www.pwc.dk

EG Danmark A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls as at 14 June 2024 in relation to EG Danmark A/S's development and operating services for Mainmanager

October 2024

pwc

Contents

1 Management's statement

The accompanying description has been prepared for customers who have used EG Danmark A/S's development and operating services for Mainmanager and its 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.

EG Danmark A/S uses team.blue Denmark A/S as subservice suppliers of housing, network, virtual server and storage services. This report uses the carve-out method and does not comprise control objectives and related controls that team.blue Denmark A/S perform for EG Danmark A/S.

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

EG Danmark A/S confirms that:

a) The accompanying description in section 3 fairly presents EG Danmark A/S's development and operating services for Mainmanager that have processed customers' transactions as at 14 June 2024. The criteria used in making this statement were that the accompanying description:

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

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and implemented as at 14 June 2024. The criteria used in making this statement were that:

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

(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.

Ballerup, 4 October 2024
EG MainManager

Signed by:
Guðrún Rós Rós Jónsdóttir
3961919E541E459...
Guðrún Rós Jónsdóttir
Director

pwc

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

Independent service auditor's ISAE 3402 assurance report on IT general controls as at 14 June 2024 in relation to EG Danmark A/S's development and operating services for Mainmanager

To: EG Danmark A/S, EG Danmark A/S's customers and their auditors

Scope

We have been engaged to provide assurance about EG Danmark A/S's description in section 3 of its IT general controls in relation to EG Danmark A/S's development and operating services for Mainmanager which has processed customers' transactions as at 14 June 2024 and about the design of controls related to the control objectives stated in the description.

EG Danmark A/S uses team.blue Denmark A/S as subservice suppliers of housing, network, virtual server and storage services. This report uses the carve-out method and does not comprise control objectives and related controls that team.blue Denmark A/S perform for EG Danmark A/S.

Some of the control objectives stated in EG Danmark A/S's description in section 3 can only be achieved if the complementary controls at the customers are suitably designed together with EG Danmark A/S's controls. This report does not comprise the suitability of the design of these complementary controls.

We have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon

EG Danmark A/S's responsibilities

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

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on EG Danmark A/S's description and on the design of controls related to the control objectives stated in that description, based on our procedures.

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

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its development and operating services for Mainmanager and the design 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. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by EG Danmark A/S in the Management's statement section.

As mentioned above, we have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon. 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

EG Danmark A/S'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 Danmark A/S's development and operating services for Mainmanager that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

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

a) The description fairly presents how IT general controls in relation to EG Danmark A/S's development and operating services for Mainmanager were designed and implemented as at 14 June 2024;

b) The controls related to the control objectives stated in the description were suitably designed as at 14 June 2024.

Description of test of controls

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

pwc

Intended users and purpose

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

Aarhus, 4 October 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Signed by:
Jesper P. M
188335E51B46430...

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

3 Description of processing

Introduction and scope

This system description concerns the IT general controls related to application development and hosting activities at EG Danmark A/S, which is owned by the private equity fund Francisco Partners. Standard IT operations and hosting activities are provided by EG CloudOps, and application development is handled by Örn Software ehf. (an EG Company), which in this report are referred to as EG.

As far as application development is concerned, EG works according to the same procedures and methods on all development tasks.

EG uses team.blue Denmark A/S and B4Restore A/S as subservice suppliers of physical security in data centres where customer operations are performed. team.blue Denmark A/S is e.g. responsible for physical security, hardware, network, backup, hypervisor and storage.

This report uses the carve-out method and does not comprise controls performed by subservice suppliers team.blue Denmark A/S. For 2023, these controls are covered by auditor's reports received from the sub-service suppliers.

EG handles operation and monitoring in connection with IT operations and hosting activities and 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.

This description is limited to general standards of administration as described in EG's standard contract. Specific matters related to individual customer contracts are not covered.

Based on the above delimitation and the system description specified below, EG assesses that we have maintained effective controls in all material matters. EG is aware of the continuous development in the area and continuously works to improve the controls.

Description of services covered by the report

The services provided by EG are tailored to several different types of customers. The conditions for the individual customers are specified in contracts; each business area is based on standard contracts which may contain individual adjustments and options. The following areas cover the services offered by EG:

- Hosting
- Application development
- Consulting
- Implementation

EG delivers the following solutions and modules to the customers:

EG MainManager

Control environment

Management structure

Compliance with the requirements in relation to IT security follows the organisation established in relation to the management of information security as described below.

At EG, the organisational set-up and management are based on a structure by function where the manager of the individual department has staff responsibilities. The security responsibility of the individual processes is delegated to the individual(s) responsible and to the performing individual(s), respectively. The manager responsible has the responsibility of ensuring that the process is followed and documented by the performing employees.

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 and CISO and the head 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.

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 VP of Corporate IT is responsible for the operations in accordance with established guidelines and for the day-to-day management.

The employees' day-to-day manager is responsible for checking that the employee complies with group-related policies and procedures that support the IT security policy as well as with local guidelines and procedures.

Security incidents, status and security weaknesses are reported to the IT security committee which initiates any further action.

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 version 8.

The overall security framework at EG consists of:

- The cyber and information security policy
- Group-related policies, procedures and guidelines that apply to all EG companies and are available in EG's information security system for all employees
- Local security procedures and instructions in the individual business units or at EG companies.

The IT security committee performs an annual assessment 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. At the same time, the committee assesses whether there is a need for a renewed risk assessment.

Human resource 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 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.

The individual employee is responsible for complying with the IT security policy 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 established procedures. If an employee become 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.

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.

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.

The areas of the buildings are divided into the following sections:

1. Public areas (canteen, staircases, reception and external meeting rooms): 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.

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

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.

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 compliance with the guaranteed availability of systems. The aim is to minimise the time it takes to restore normal operations. To accommodate this, the company works with preventive monitoring and related corrective actions. With this method, there is no or minimal impact on 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 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

Segregation of duties is the fundamental principle at personal as well as organisational level.

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.

Backup data is stored separately from production data in accordance with the principles of segregation of duties.

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 is used.

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.

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 only takes place if stated in the agreement with the customer.

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 from outside takes place using two-factor authentication by SMS passcode or similar.

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.

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

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

EG is responsible for patch management on systems in the data centres. The purpose is to ensure that security updates are installed on critical systems. This applies to systems used internally as well as systems used by external customers (customer systems).

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.

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.

According to the security policy, security tests must be performed as required.

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.

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.

Development is driven by both in-house initiatives and customer input. A fixed process/template provides the foundation of our work; this process/template may vary according to the size and complexity of each individual task.

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.

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 a disaster recovery plan which describes 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.

Complementary controls

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.

The detailed control objectives and control activities, including tests, are addressed in the table.

Improvements

In 2023, EG has taken the following measures to improve the level of security and data protection:

Month	Measures
June 2023	Appointment of new CIO at EG Danmark A/S with responsibility for EG Corporate IT.
September 2023	Revised Security Incident Management Policy.

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 and implementation of the controls has included the control objectives and related control activities selected by Management and listed in section 0. Any other control objectives, related controls and controls at customers are not covered by our test actions.

4.2 Test actions

The test actions performed when determining the design 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 have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed.

4.3 Control objectives, control activity, tests and test results

Control objective 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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have made inquiries of Management about the procedures/control activities carried out. We have verified that Management has approved the security policy and that the policy is subject to review at least once a year. We have also verified that the policy is easily accessible to the employees.	Our test has shown that not all policies and procedures have been updated and approved within the last year. We have been informed that this is due to transfer of operations to EG CloudOps. No further exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have discussed information security management in general terms with Management. We have verified that the organisational responsibility for information security has been documented and implemented. By inspection, we have furthermore checked that non-disclosure agreements, reporting on information security incidents and records of assets have been prepared.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have made inquiries of Management about the procedures/control activities carried out. We have verified that adequate procedures for collaboration with external suppliers have been established. Through random sampling, we have also checked that cooperation with external parties is based on approved contracts.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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, e.g. in case of servicing of firefighting and cooling systems.	We have 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 have moreover reviewed employees with access to secure areas and verified that documented Management approval has been granted.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
Securing offices, rooms and facilities For all server rooms, an access control system has been installed to ensure that access is restricted to employees approved by Management. Review of existing access rights is carried out once a year and in case of changes. The security policy specifies a procedure for working in secure areas. It also specifies that access points such as delivery and loading areas where unauthorised individuals can obtain access to the area are limited and that access is only granted to identified and approved individuals. Servicing of all relevant supporting equipment such as firefighting, cooling and UPS is logged. 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.	We have made inquiries of Management about the procedures performed. We have inspected all server rooms and verified that access routes have been secured by use of a card reader. Through random sampling, we have checked that periodic reviews are performed.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
Siting and protection of equipment Data centres are protected from environmental disasters such as fire, water and heat. Server rooms are further secured with armoured glass. Safety and maintenance are regularly tested in collaboration with service providers such as G4S, FireEater and DBI. The security policy specifies that access to equipment and cables can only be obtained with security clearance or in the company of EG IT or other EG staff approved by IT. Data centres are operated by third parties.	We have made inquiries of Management about the procedures/control activities carried out. By inspection, we have reviewed the operating facilities and have verified 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.
Supporting utilities (security of supply) Data centres are protected from power failure by use of UPS (uninterruptible power supply) and emergency power facilities. These facilities are tested at regular intervals according to the test plan. The facilities are also tested at regular intervals in collaboration with the supplier. Data centres are operated by third parties.	We have 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.
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.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
Control objective D: Communications and operations management *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.*		
Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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. NTP is used for time synchronisation.	We have 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 have also verified that adequate monitoring and follow-up on this are performed.	Our test has shown that not all procedures have been updated and approved by management within the last year. We have been informed that this is due to transfer of operations to EG CloudOps.No further exceptions noted.
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.	We have made inquiries of Management about the procedures/control activities carried out. We have reviewed 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.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
• 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 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.		
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 have 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.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have 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. We have reviewed the procedure for external storage of backup tapes to confirm that backups are stored safely.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have 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 have verified that logging parameters are set up to ensure that actions performed by users with extended access rights are logged. Through a random inspection, we have furthermore checked that adequate follow-up on logs from critical systems is performed.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have made inquiries of Management about the procedures/control activities performed and reviewed the procedure for handling incidents. Through a random inspection, we verified 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.

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.*

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have made inquiries of Management about the procedures/control activities carried out. We have reviewed 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.
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 have made inquiries of Management about procedures/control activities carried out in connection with password controls, and we have verified 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 verified that company systems are accessed on the basis of username and password.	No exceptions noted.

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.*

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have 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 verified that identified deviations are subject to remedial action.	No exceptions noted.
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 have 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.
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.	We have made inquiries of Management about the procedures/control activities carried out, and we have verified 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.	No exceptions noted.

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.*

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
SMS passcode, token 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.	By inspection, we ascertained that the network is segmented into smaller networks using VLANs and DMZs to reduce the risk of unauthorised access.	
Management of network connections Every six months, 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 only take place through security-cleared solutions. Guests must use EG's guest network.	We have 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.

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.*

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have made inquiries of Management about the procedures/control activities carried out in order to limit access to information. We have reviewed 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.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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 have made inquiries of Management about the procedures/control activities carried out in order to maintain separation of the individual environments. By inspection, we have verified that changes are tested in the test environment. Through a random inspection, we reviewed changes made during the period and verified that the changes have been documented.	No exceptions noted.
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	We have 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.	During our test, we have seen that for 2 out of the sampled changes, segregation of duties had not been enforced. No further exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
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. Changes to customer-specific systems are recorded as incidents in the help desk system. This includes e.g. information on date, status and follow-up comments. Emergency changes to operating systems and networks that bypass the normal business process are tested and approved subsequently.	Furthermore, we have ascertained 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.	
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. 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. Development, test and operating environments are segregated. All environments are subject to security requirements.	We have made inquiries of Management about the procedures/control activities performed and have reviewed the adequacy of the change management procedures being part of the release and deployment management. We have verified that an appropriate change management system has been implemented and is supported by technical infrastructure.	No exceptions noted.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
Release management applications EG performs release management. Releases are made on an as-needed basis and often several times a week. 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. According to EG's project model, safety is ensured in all development phases. For each release, the following is ensured: • Traceability with respect to each item of the release contents • 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	We have 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.

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.

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
• Presence of roll-back plans for releases • Communication of new releases to customers.		
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 have 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.

Control objective G: Disaster recovery plan

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

Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
Structure of disaster recovery The overall disaster recovery plan consists of a high-level disaster recovery procedure as well as operational disaster recovery plans for the specific disaster areas which aim to ensure continuity in critical situations. The operational disaster recovery plan includes a description of the disaster 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 disaster recovery** Annually, a test is performed of disaster recovery comprising desktop tests and realistic test scenarios. Parts of the contingency plan are tested according to a test plan. Where relevant, this includes real-time testing.	We have made inquiries of Management about the procedures/control activities carried out. We have reviewed the materials provided on disaster recovery, and we have verified that the organisational and operational IT disaster recovery plan includes management function descriptions, contact information, notification lists as well as instructions.	No exceptions noted.