ROESGAARD

NÅR OVERBLIK SKABER VÆRDI

Enreach Campaigns A/S

ISAE 3402 type 2 assurance report on IT general controls related to Flows by Enreach for the period from 1 September 2024 to 31 August 2025

Contents

Section 1: Enreach Campaigns A/S' statement

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

Enreach Campaigns A/S is using the subservice organisations Global Connect A/S, Digital Reality, Amazon Web Services and Microsoft Azure. This assurance report is prepared in accordance with the partial method and Enreach Campaigns A/S' description does not include control objectives and controls within Global Connect A/S, Digital Reality, Amazon Web Services and Microsoft Azure. Certain control objectives in the description can only be achieved if the subservice organisations controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subservice organisations.

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

Enreach Campaigns A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Enreach Campaigns A/S' Flows by Enreach processing of customer transactions throughout the period from 1 September 2024 to 31 August 2025. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The type of services provided
- The procedures within both information technology and manual systems, used to manage IT general controls
- Relevant control objectives and controls designed to achieve these objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

(ii) Contains relevant information about changes in the IT general controls, performed during the period from 1 September 2024 to 31 August 2025.

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers

and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period from 1 September 2024 to 31 August 2025 if relevant controls with the subservice organisation were operationally effective and the customers have performed the complementary controls, assumed in the design of Enreach Campaigns A/S' controls during the entire period from 1 September 2024 to 31 August 2025. The criteria used in making this statement were that:

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

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

(iii) The controls were used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, during the period from 1 September 2024 to 31 August 2025.

Hvidovre, 9. Januar 2026
Enreach Campaigns A/S

Casper Langhoff
CEO

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

To Enreach Campaigns A/S, their customers and their auditors.

Scope

We have been engaged to report on a) Enreach Campaigns A/S' description in Section 3 of its system for delivery of Enreach Campaigns A/S' Flows by Enreach throughout the period from 1 September 2024 to 31 August 2025 and about b)+c) the design and operational effectiveness of controls related to the control objectives stated in the description. Enreach Campaigns A/S is using the subservice organisations Global Connect A/S, Digital Reality and Amazon Web Services. This assurance report is prepared in accordance with the partial method and Enreach Campaigns A/S' description does not include control objectives and controls within Global Connect A/S, Digital Reality and Amazon Web Services. Certain control objectives in the description can only be
achieved if the subservice organisation's controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subservice organisations. Some of the control objectives stated in Enreach Campaigns A/S' description in Section 3 of Flows by Enreach, can only be achieved if the complementary controls with the customers have been appropriately designed and works effectively with the controls with Enreach Campaigns A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Enreach Campaigns A/S' responsibility

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

Roesgaard's independence and quality control

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

Auditor's responsibility

Our responsibility is to express an opinion on Enreach Campaigns A/S' description (Section 3) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively. An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation in Section 3.

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

Limitations of controls at a service organization

Enreach Campaigns A/S' description in Section 3, is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

Opinion

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

a) The description of the IT general controls, as they were designed and implemented throughout the period from 1 September 2024 to 31 August 2025, is fair in all material respects.
b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 September 2024 to 31 August 2025 in all material respects, if controls with subservice organisations were operationally effective and if the customers have designed and implemented the complementary controls assumed in the design of Enreach Campaigns A/S' controls throughout the period from 1 September 2024 to 31 August 2025
c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period from 1 September 2024 to 31 August 2025.

Description of tests of controls

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

Intended users and purpose

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

Horsens, 9. januar 2026

Roesgaard
Godkendt Revisionspartnerselskab

Michael Mortensen
Partner, Statsautoriseret revisor

Section 3: Description of Enreach Campaigns A/S' services in connection with the operating of Flows by Enreach

Introduction

The purpose of this description is to supply information to Enreach Campaigns' customers and their stakeholders (including auditors) regarding the requirements in the International Standard for Assurance Engagements on controls at a service organisation, ISAE 3402.

Additionally, the purpose of this description is to provide information on our information security code of practice which is applicable for our delivery of the product and service Flows by Enreach to our customer.

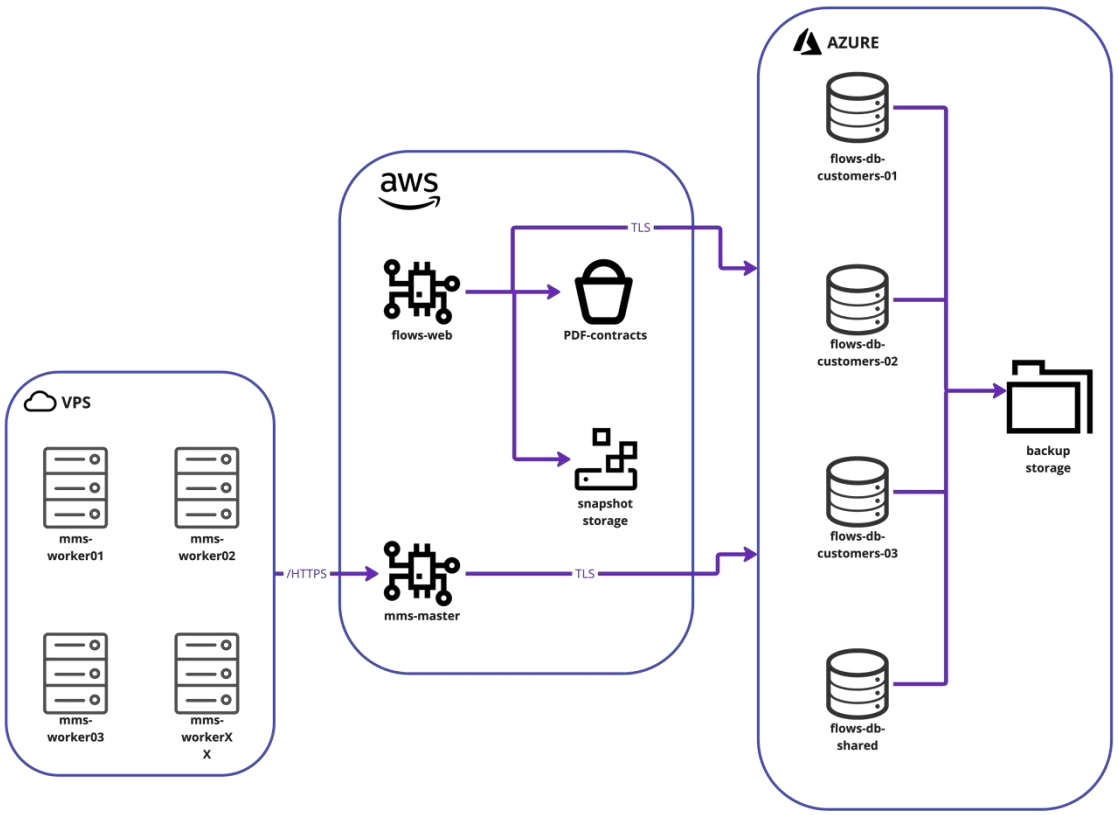
The description comprises the control areas and controls regarding Flows by Enreach, which cover the majority of our customers and are based on our standard delivery. Individual customer relations are not included in this description.

Enreach Campaigns and our software Flows by Enreach

Enreach Campaigns is a Danish IT company based in Hvidovre. We develop, host, and supply software in the form of a SaaS solution to contact centres. One of our core products is supplying the software Flows by Enreach (here-after just named "Flows"), which is supplied as a SaaS-solution, which means it is hosted in our own data centres and is based on a flexible and scalable subscription-based model.

Technical setup and placement

Flows is a web application based on .NET (the primary language is C#) and with a frontend based on e.g. JavaS- cript and MVC. The database technology is MSSQL, and hosting is via the Danish data centres GlobalConnect (Taastrup) and Digital Reality (Ballerup) as well as AWS' (Amazon Web Services) and Microsoft Azure. Frankfurt and Dublin locations, and Enreach's European based data centres. The only AWS locations we have chosen services in, and where data thereby is located in, are AWS' Dublin site in Ireland and AWS' site in Frankfurt, and thereby no data in Flows leaves the EU. Our infrastructure and architecture are designed in such a way that there is redundant failover equipment for everything from firewalls and switches to database and web servers. Most of the equipment is also placed in both data centres, which means that one location can resume operations, if another location is impacted by reduced access or other problematic circumstances, internal as well as external.



Organisation and responsibility
Enreach Campaigns employs 23 persons in Denmark, Sweden, Ukraine, the UK, and Finland. About half the employees are placed in Denmark and have their daily workplace at the office in Hvidovre.

The management consists of an ultimately responsible Managing Director, and his direct report are Finance Manager (UK), Head of Tech (DK), Head of Growth (UK), and Head of Customer Relations (DK).

The Tech department, led by the Head of Tech, consists primarily of developers in a "DevOps" constellation, where two persons are dedicated to operations, optimising servers and infrastructure, monitoring and handling operational issues, but where all have operations as their first priority in case of technical issues on the platform.

The developers are organised in frontend and backend expertise, with a chief architect who makes the general decisions on language, technology, and new frameworks on the basis of a thorough analysis and in cooperation with the Head of Tech. In addition, a network administrator is responsible for network and telephony, whereas a project manager and tester have a close cooperation with Enreach Campaigns' other departments.

Management has the overall responsibility for IT security and that the company's general IT security policy is observed.

Next to the daily organisation based on function, a security organisation has been organised with an Information Security Committee comprising key employees from various parts of Enreach Campaigns, including management, and an information security coordinator who has the daily, operational responsibility for a number of tasks defined in Enreach Campaigns' information security code of practice. The information security coordinator is additionally responsible for all employees being aware of the information security manual, including rules and procedures, helps them to access and understand it, and acting on and observing the rules. In conclusion, the responsibility for a variety of matters related to the business systems that support the daily work with supplying the product and service flows is delegated to the system owners.

Risk management in Enreach Campaigns A/S
Risk management in Enreach Campaigns A/S is done for all areas connected with delivering the product and service Flows, and which thereby may have financial consequences for our customers. Risk analysis, assessment, and management are based on ISO 27005, and are based on impact analyses and vulnerability analyses at service level. Service is understood as business systems supporting the delivery of Flows as well as Flows in itself as a customer system.

The business in Enreach Campaigns answers the questions in the impact analysis, while the IT department in Enreach Campaigns performs the vulnerability analysis.

Risk analyses are conducted as consequence and vulnerability analyses at least annually, after which the collected security overview is brought up for the information security committee and finally Enreach Campaigns' management, for the definition of further actions.

Generally, on our control objectives, including rules and procedures as well as implemented controls
Working procedures and processes connected with the supply of the product and service Flows are based on our information security code of practice, on top of which are defined procedures and controls with associated contingency plans etc.

The framework for the information security code of practice is ISO 27001, and the code of practice is classified according to the following control areas:

- Information security management and security policy
- Organisation of information security
- Human resource security
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management

- Information security aspects of business continuity management
- Compliance

Information security management and security policies
Enreach Campaigns' general information security policies are prepared for the purpose of ensuring a continuous embedding of working methods, principles, and routines that comply with the determined security level.

The information security policies must be observed in all regards and aims to ensure a secure and stable delivery of the product and service Flows, including compliance with relevant legislation, such that all significant risks of breakdowns, data theft, and data breaches are reduced.

The policies are reviewed and approved annually. The information security coordinator is the management's and information security committee's "auxiliary arm" in the daily embedding of the policies, and this ensures communication on an ongoing basis to all relevant parties.

Organisation of information security

Segregation of duties
We have a clear and well-defined organisation with segregation of duties, which entails that dependency on key persons is reduced as much as possible. In addition, segregation of duties has been introduced to areas where there is a risk of the occurrence of misuse of the company's data and information.

Equipment and teleworking
We have a policy for the use of mobile devices and home workplaces/remote workplaces. Minimum requirements have been defined for the protection of all devices, as well as access to business systems and data. All devices must be protected by antivirus and firewall and must be enrolled in InTune (exept mobile phones). A number of system accesses to Enreach Campaigns' business systems require VPN access. These are issued and installed by the IT department (approval by the Head of Tech, issuing and configuration of an employer in the IT department). VPN can be installed on PCs supplied and owned by Enreach Campaigns, but never on privately owned PCs.

Human resource security
We have defined a number of procedures that ensure security prior to, during, and, if relevant, after employment.

Procedures concerning processes before a potential employment ensure that potential employees are screened and that relevant matters are checked within the framework of current legislation.

All employees must adhere to a number of terms regarding confidentiality about own, Enreach Campaigns', and customers' matters. This is described in each employee's employment contract.

During employment it is ensured between the employee, the immediate manager, and the information security coordinator that the employee is kept up to date regarding and complies with aspects regarding information security.

We have procedures that ensure that employees at the termination of employment cannot cause damage to Enreach Campaigns, or the system Flows by means of immediately removing rights to business systems and check this.

In addition, a number of sanctions have been defined, in case information security is breached or disregarded.

Access management
We have a string of procedures that ensure that access control and the allocation of rights occur in compliance with the established security level.

Only employees with a work-related need for having access to systems and data are granted access to the concerned business systems and associated data.

The heads of department are responsible for access rights being granted on the basis of a work-related need and in consideration of regulatory and contractual obligations.

We have a number of controls that ensure that this occurs on an ongoing basis, and that all access corresponds to the work-related needs in each function and for each employee.

We have defined a string of requirements for the protection of all devices (PCs, mobile phones, tablets) as well as passwords in all business systems. Employees are trained and checked within these areas.

We have a number of procedures that ensure that only a group of privileged employees has access to system administrator tools, central servers (e.g. domain controller), source code etc.

Production servers and other servers containing production data and customer data are only present in Enreach Campaigns' data centres (physical and cloud) and not at any office locations. Only specially trusted employees with a work-related need have access to the data centres. These accesses are assessed and inspected regularly via onboarding, offboarding procedures and ad hoc controls.

Cryptography
We have procedures for the use of cryptography, including the generation and management of encryption keys and certificates.

This means, i.a, that Flows must have a valid SSL certificate, which Enreach Campaigns verifies, such that data exchange only occurs in a secure and encrypted manner (through HTTPS). SSL-certificates are managed solely by the IT department, where the application architect and network administrator are responsible for SSL certificates. No certificates may be acquired or issued bypassing these.

This requirement concerns access to Flows through the user interface and through API alike.

Physical and environmental security
Servers are only placed in data centres provided by suppliers who have been issued, and annually can show, assurance reports at the level of ISAE 3402.

Enreach Campaigns' office premises are subject to a number of procedures that secure the office as well as material and units stored at the office, regardless of servers only being placed in data centres.

This entails, i.a, procedures aimed at employees describing security measures for offices, common areas, and similar areas.

Operations security

Operating procedures and monitoring
We have operating procedures for the IT department's most significant duties, and these procedures are subject to versioning and change management.

We have defined the responsibility for ensuring that an assessment of the capacity requirements for critical IT systems are monitored continuously and alerts are acted upon.

The IT department, led by the Head of Tech, consists primarily of developers in a "DevOps" constellation, where two persons are dedicated to operations, optimising servers and infrastructure, monitoring and handling operational issues, but where all have operations as the first priority in case of technical issues on the platform or information security issues.

All instances of Flows are monitored by means of monitoring tools.

Critical levels and values are defined for all these monitoring areas. Alarms must trigger when these values are reached and must be sent to key employees either via email (for less critical alerts) or SMS (critical alerts).

Historical logs and events are reviewed in a structured manner when planning improvements and optimisation.

Development of Flows, management, and quality assurance
The development of Flows, including release of changes, occurs according to Enreach Campaigns' formalised and embedded development model.

The development process is Enreach Campaigns' own method derived from an agile approach to development, SCRUM, and RUP. The development takes place in sprints, but not of an eternal, specified duration, as sprints are defined according to prioritised tasks in backlog.

Next to master releasees, hot fix releases are performed with corrections of distinct errors and significant inexpediencies. Disclosed security weaknesses with the priority of 1 (cf. Enreach Campaigns' operations procedure) must always be handled as quickly as possible, and no later than within 5 working days.

Development occurs in development environments where code is branched from the main branch/"default". These development branches are connected with the staging database, where test data is found. Test data and production data are thus completely segregated, and customers' data must not be copied from master to staging without approval from the Head of Tech. If this permission is granted, it can and will only comprise configuration data in order to test and develop up against true, complex data in order to ensure the quality of the development, but it must and can never comprise data on the customer's prospects, employees or similar.

Function testing takes place in development branches (also called feature branches), after which code is tested and merged to pre-production branches, from which code is tested again prior to finally deployed for production.

Logging
We have procedures concerning the scope, processing, protection, and check of logging on various system types.

All logins and significant user actions in Flows are monitored and logged. The logging of significant user actions concerns i.a. data export.

All changes to data are registered.

Communications security
We have procedures for network management and monitoring, including maintenance of network and network equipment.

Traffic on all connections and interfaces are monitored in relation to data volume over periods of time. Alarms have been set up that are triggered and sent to technical personnel in case of abnormalities (traffic spikes, significant delays between master databases and slave databases, and much else).

Exchange of information solely occurs by means of secure connections. If this occurs via the public Internet, data is encrypted (in principle by means of HTTPS). via LAN.

Systems acquisition, development, and maintenance
We have procedures that ensure secure change management in business supporting systems. The procedures prescribe i.a. that change logs are obtained and evaluated, and that changes are tested before they are released.

As all significant internal work processes are documented, the process documentation is updated where necessary, in connection with changes.

Please note that this section and the procedures referred to herein concern maintenance and changes in business supporting systems, not the solution Flows itself. Procedures and principles for changes in Flows are described in a previous, separate section.

Supplier relationships
In all cooperation agreements with suppliers, we have defined security requirements and minimum requirements for the services provided to us by the supplier.

We have ensured that the matters we base our agreement on regarding the use of the product and service Flows in relation to customers, are in accordance with our requirements to our suppliers.

We regularly, and at least annually, review the assurance reports for the entered agreements.

Information security incident and event management
The information security committee has defined procedures for information security incidents and events, which are embedded in Enreach Campaigns and which the management is responsible for being observed.

We define information security incidents as:

- The detection of successful external and unwanted intrusion in systems
- Finding customer data (hosted in the master database for Flows) online, where there is an obvious or strong suspicion that the publication of data has not occurred with the customer's approval and intent
- Finding data on current or former employees in Enreach Campaigns online, where publication of data has occurred without Enreach Campaigns' involvement or intent
- Finding other confidential business data online (according to the same directions) defined as customer contracts, revenue, or information which is classified as secret according to further definition by the information security committee

We define information security events as:

- Events that, if they had not been discovered, could have led to security incidents
- Situations where unintended data or information by accident (due to human error) has been sent to other recipients than the intended, and that it is assessed that this may entail damage or serious consequences for Enreach Campaigns

Procedures have been defined for both, which describe for employees and managers how they should act in case of incidents and events, including (but not limited to) collecting evidence and contact with authorities, if necessary.

Information security aspects of business continuity management
We have defined the responsibility for preparing and maintaining contingency plans.

We have established adequate redundancy to meet the requirements for availability and the guarantees for up- time that we have agreed in contracts with our customers.

All members of the DevOps team have been trained in the plans.

Plans and procedures are reviewed after each operational issue, where human action has been necessary to re-establish operations on parts of the platform.

Compliance
Information security is subject to annual audit by an independent external IT auditor

Significant changes in IT-environments
There have been no significant changes to IT-environments in the period.

Complementary controls
Regarding our customers, Enreach Campaigns is responsible for delivering the services and the operations described in the contract concerning Flows between the customer and Enreach Campaigns.

Matters not comprised by the contract are the customer's own responsibility.

Creation of users, protection of user information, and secure login procedures are the responsibility of the customer. The customer can enable MFA login on users in Flows. Enreach Campaigns recommends our customers to do this to the extent it is possible for the customer, in order to protect the customer's data and activities in Flows.

Changes in the audit period
No significant changes in the period.

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

Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages.

To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This statement is issued according to the partial method and therefore does not include controls of Enreach Campaigns A/S' subservice organisations.

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

We performed our test of controls at Enreach Campaigns A/S by the following actions:

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

Test results

Below, we have listed the tests performed by Roesgaard as basis for the evaluation of the IT general controls with Enreach Campaigns A/S.

A.5 Information security policies			
A.5.1 Management direction for information security **Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
5.1.1	*Policies for information security* A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.	We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant external parties.	No deviations noted.
5.1.2	*Review of policies for information security* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inspected that the information security policy has been reviewed and approved by management.	No deviations noted.

A.6 Organisation of information security			
A.6.1 Internal organisation **Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected an organisation chart showing the information security organisation. We have inspected the description of roles and responsibilities within the information security organisation.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.	We have inspected documentation for segregation of duties. We have inspected general organisation chart for the organisation.	No deviations noted.
A.6.2 Mobile devices and teleworking **Control objective: To ensure the security of teleworking and use of mobile devices**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
6.2.1	*Mobile device policy* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected policy for securing of mobile devices. We have inspected, that technical controls for securing of mobile devices have been defined. We have, by sample test, inspected that mobile devices have technical controls implemented.	No deviations noted.

6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected the policy for securing of remote workspaces. We have inspected the underlying security measures for protection of remote workspaces.	No deviations noted.
A.7 Human ressource security			
A.7.1 Prior to employment **Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
7.1.1	Prior to employment Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered	We have inspected the procedure for screening new employees. We have inquired about screening of new employees during the period. We have inspected sample documentation.	No deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities in information security.	We have inspected the procedure for onboarding new employees. We have inspected documentation that new employees have been informed about their roles and responsibilities in information security.	No deviations noted.

A.7.2 During employment **Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inspected the information security policy regarding the setting of requirements for employees and contractors.	No deviations noted.
7.2.2	*Information security awareness education and training* All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inspected that activities to develop and maintain employees' security awareness have been carried out. We have inspected documentation that all employees have completed the awareness training provided.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected that a formal disciplinary process has been established and communicated to employees and contractors.	No deviations noted.

A.7.3 Termination and change of employment **Control objective: To protect the organisation's interests as part of the process of changing or terminating employment**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inspected that there are procedures, ensuring that accesses are revoked. We have inspected that the applicable duty of confidentiality is stated in employment contracts for employees terminated during the period. We have, by sample test, inspected that the offboarding procedure has been followed for resigned employees.	No deviations noted.

A.9 Access control			
A.9.1 Business requirements of access control **Control objective: To limit access to information and information processing facilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inspected the access control policy. We have inspected that the policy has been reviewed and approved by management.	No deviations noted.

9.1.2	*Access to network and network services* Users are only being provided with access to the network and network services that they have been specifically authorized to use.	We have inspected that a procedure has been established for allocating access to networks and network services. We have inspected extracts of users with access to networks and network services has a work-related need.	No deviations noted.
A.9.2 User access management **Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected that formalised procedures for user registration and de-registration have been established.	No deviations noted.
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services	We have inspected that a procedure for user administration has been established.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected the procedures for allocation, use and restrictions of access rights. We have inspected, that periodical review of privileged access rights is being performed.	No deviations noted.

9.2.4	*Management of secret-authentication information* *of users* The allocation of secret authentication information is controlled through a formal management process.	We have inspected the procedure regarding allocation of access codes to platforms. We have inspected documentation that the password policy is implemented in systems used to manage secret authentication information about users.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals	We have inspected the procedure for regular review and evaluation of access rights. We have inspected that a review and evaluation of access rights is carried out during the period.	No deviations noted.
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that resigned employees have had their access rights cancelled.	No deviations noted.

A.9.3 User responsibilities **Control objective: To make users accountable for safeguarding their authentication information**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
9.3.1	*Use of secret authentication information.* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected guidelines for use of secret passwords. We have inspected, the implemented password policy.	We have been informed that the strength of the password functionality in Flows does not live up to current standards. No further deviations noted.
A.9.4 System and application access control **Control objective: To prevent unauthorised access to systems and applications**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
9.4.1	*Information access restriction* Access to information and application system functions has been restricted in accordance with the access control policy.	We have inspected policies and procedures to ensure the restriction of access to the functions of application systems. We have inquired how it is determined whether the users have a work-related need.	No deviations noted.
9.4.2	*Secure logon procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected the procedure for secure logon. We have inspected, that MFA has been established in connection with logon.	No deviations noted.

9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inspected that policies or procedures set requirements for the quality of passwords. We have inspected that the systems for managing passwords are set up in accordance with the requirements.	No deviations noted.
9.4.5	*Access control to program source code* Access to program source code has been restricted.	We have inquired into procedures for restricting access to program source codes. We have inspected that access to source codes has been restricted.	No deviations noted.
A.10 Cryptography			
A.10.1 Cryptographic controls **Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy for the use of encryption. We have inspected that transmission over the internet is done with a secure connection.	We have found that Flows supports outdated encryption protocols. No further deviations noted.
10.1.2	*Key Management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, which supports the company use of cryptographic techniques. We have inspected that cryptographic keys are active, and that their renewal is being followed up on.	No deviations noted.

A.11 Physical and environmental security			
A.11.1 Secure areas **Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected the procedure for physical protection of facilities and perimeter security. We have inspected that access to locations with equipment is limited to employees who need the access.	No deviations noted.
A.11.2 Equipment **Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
11.2.1	*Equipment sitting and protection* Equipment is sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.	We have inspected the procedure regarding the placement and protection of equipment. We have inspected that access to locations with equipment is limited to employees with a work-related need.	No deviations noted.
11.2.7	*Secure disposal or re-use of equipment* All items of equipment containing storage media have been verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.	We have inquired into the procedure for deletion of data and software on storage media, before disposing of same.	No deviations noted.

11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	We have inspected the procedure for ensuring the protection of unattended equipment. We have inspected documentation of the implementation of a blank screen.	No deviations noted.
A.12 Operations security			
A.12.1 Operational procedures and responsibilities **Control objective: To ensure correct and secure operation of information processing facilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
12.1.1	*Documented operating procedures.* Operating procedures have been documented and made available to all users.	We have inspected that documentation for operating procedures is updated and accessible to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure for changes in information processing facilities and systems. We have, by sample test, inspected documentation that change requests are being managed according to the established procedure.	No deviations noted.
12.1.3	*Capacity management* The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inspected the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements.	No deviations noted.

12.1.4	*Separation of development-, test- and operations facilities.* Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.	We have inspected the process & technical documentation that used system environments have been separated.	No deviations noted.
A 12.2 Protection from malware **Control objective: To ensure that information and information processing facilities are protected against malware**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inspected that antivirus software has been installed on the systems and databases used for the processing of personal data. We have also inspected that the antivirus software is up to date.	No deviations noted.
A.12.3 Backup **Control objective: To protect against loss of data**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
12.3.1	*Information backup* Backup copies of information software and system images are taken and tested annually in accordance with an agreed backup policy.	We have inspected documentation that the procedure for back-up has been reviewed and updated during the period. We have by sample test, inspected that backups are taken according to the procedure. We have inquired about ongoing testing of backup.	No deviations noted.

A.12.4 Logging and monitoring **Control objective: To record events and generate evidence**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inspected procedures for logging of user activities. We have walked through the use of logging at the audit meetings.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inspected procedures for securing log information. We have inspected that access to logging information is restricted.	No deviations noted.
A.12.5 Control of operational software **Control objective: To ensure the integrity of operational systems**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inspected the procedure for patching and upgrading systems and that it has been reviewed and updated during the period. We have inquired about the process flow routines.	No deviations noted.

A.12.6 Technical vulnerability management **Control objective: To prevent exploitation of technical vulnerabilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inspected that malware protection checks have been performed during the period. We have inspected that systems are patched. We have enquired documentation about technical vulnerabilities of information systems being used are obtained in a timely fashion.	We have not been able to obtain documentation about technical vulnerabilities of information systems being used are obtained in a timely fashion No further deviations noted.
A.13 Communications security			
A.13.1 Network security management **Control objective: To ensure the protection of information in networks and its supporting information processing facilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inspected that there are defined requirements for the management and control of networks. We have walked through the process of monitoring and use of controls to protect the systems and data.	No deviations noted.

13.1.2	*Security of network services* Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided inhouse or outsourced.	We have inspected that evaluation of the suppliers services is performed and walked through the choices of suppliers at the audit.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected technical documentation that system environments are being segregated.	No deviations noted.
A.14 Aquisition, development and maintenance of systems			
A.14.1 Security requirements of information systems **Control objective: To ensure that information security is an integrated part of information systems through the entire lifecycle. This also includes requirements of information systems, rendering services on public networks**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
14.1.1	*Information security requirements analysis and specification* The information security related requirements are being included in the requirements for new information systems or enhancements to existing information systems.	We have inspected the procedure for software development. We have inspected documentation that the procedure has been reviewed and updated during the period.	No deviations noted.

A.14.2 Security, development- and supporting processes **Control objective: To ensure that information security is planned and implemented with the development life cycle**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
14.2.1	*Secure development policy* Rules for the development of software and systems have been established and applied to developments within the organisation.	We have inspected rules for developing software and systems. We have, by sample test, inspected that the rules have been followed.	No deviations noted.
14.2.2	*Change control procedures* Changes to systems within the development lifecycle are being controlled using formal change control procedures.	We have inspected that the procedure for change management contains the following requirements: • Test • Approval • System documentation We have, by sample test, inspected that implemented changes were performed according to the change management procedure.	No deviations noted.
14.2.3	*Technical review of applications after operating system changes* When operating platforms are changed business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.	We have, by sample test, inspected that changes have followed the procedure.	No deviations noted.

14.2.5	*Secure system engineering process* Principles for engineering secure systems have been established, documented, maintained, and applied to any information system implementation efforts.	We have inspected that the procedure for development of systems is established and documented. We have, by sample test, inspected that development of secure systems have followed the procedure.	No deviations noted.
14.2.6	*Secure development environment* There is established appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	We have inspected documentation that the development environment is separated from production.	No deviations noted.
14.2.9	*System acceptance testing* Acceptance testing programs and related criteria have been established for new information systems upgrades and new versions.	We have inspected that the procedure for software development contains sections about system acceptance testing. We have, by sample test, inspected that system test is an integrated part of system development.	No deviations noted.

A.14.3 Test Data **Control objective: To ensure the protection of data used for testing.**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
14.3.1	*Protection of test data* Test data are being carefully selected, protected, managed, and controlled.	We have inspected that test data is stored according to internal procedures. We have walked through the use of tools to secure test data mock and inspected a sample. We have inspected controls for ensuring that customer data are not stored locally.	No deviations noted.
A.15 Supplier relationships			
A.15.1 Information security in supplier relationships **Control objective: To ensure protection of the organisation's assets that are accessible by suppliers**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
15.1.1	*Information security policy for supplier relationships* Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets have been agreed with the supplier and documented.	We have inspected the supplier management procedure. We have inspected that the supplier policy requires that agreements entered into contain information security requirements.	No deviations noted.

15.1.2	*Addressing security within supplier agreements* All relevant information security requirements are established and agreed with each supplier that may access process store communicate or provide IT infrastructure components for the company's information.	We have inspected that the evaluation of current supplier agreements has not raised issues regarding information security requirements.	No deviations noted.
15.2 Supplier service delivery management **Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inspected that the procedure for managing suppliers and supplier agreements contains requirements of yearly monitoring and review of services rendered, are according to the contract. We have inspected, that review and assessment of relevant audit reports on significant subservice organisations have been performed.	No deviations noted.

15.2.2	*Manage changes to the third-party services* Changes in supplier services, including maintenance and improvement of existing information security policies, procedures, and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have enquired about changes of suppliers during the period.	We have been informed that there have been no changes in the use of suppliers during the period. No deviations noted.
A.16 Information security incident management			
A.16.1 Management of information security incidents and improvements **Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inspected the procedure for managing security incidents. We have inspected that the procedure has been reviewed and updated during the period.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inspected guidelines for reporting information security incidents. We have inspected that information security incidents have been reported according to the procedure.	No deviations noted.

16.1.3	*Reporting security weaknesses* Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inspected guidelines for reporting information security weaknesses. We have inquired about the weaknesses or suspected weaknesses in information systems and services.	No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inspected the procedure for assessing information security incidents. We have inquired about breaches during the period.	We have been informed that there have been no breaches during the period. No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inspected the procedure for handling information security breaches. We have inquired about breaches during the period.	We have been informed that there have been no breaches during the period. No deviations noted.
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inspected the procedure for handling information security breaches. We have inquired about breaches during the period.	We have been informed that there have been no breaches during the period. No deviations noted.

A.17 Information security aspects of business continuity management			
A.17.1 Information security continuity **Control objective: Information security continuity should be embedded in the organisation's business continuity management systems**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
17.1.1	*Planning information security continuity* Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inspected that the contingency plan includes relevant areas.	No deviations noted.
17.1.2	*Implementing information security continuity* Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	We have inspected documentation that the contingency plan is available to relevant employees. We have inquired about updating the contingency plan.	No deviations noted.
17.1.3	*Verify review and evaluate information security continuity* The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.	We have inspected documentation that risk areas in the contingency plan have been tested during the period.	No deviations noted.

A.17.2 Redundancies **Control objective: To ensure availability of information processing facilities**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
17.2.1	*Availability of information security processing facilities* Information processing facilities have been implemented with redundancy sufficient to meet availability requirements.	We have inspected the redundancy has been established to ensure availability in processing facilities.	No deviations noted.
A.18 Compliance			
A.18.2 Information security reviews **Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
18.2.1	*Independent review of information security* Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have inspected documentation that independent review of the information security has been performed.	No deviations noted.

18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inspected documentation that controls have been performed during the period.	No deviations noted.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have inspected the procedure that states the acceptable level of security patching that must be obtained.	No deviations noted

PENNEO

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

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

Casper Langhoff (CVR valideret)
Enreach Campaigns A/S CVR: 31073103
Direktør
Serienummer: e4fc44e3-48d1-42ad-b0a6-4f370c36b11c
IP: 95.166.xxx.xxx
2026-01-12 12:41:47 UTC

Mit ID

Michael Mortensen (CVR valideret)
Roesgaard Godkendt Revisionsaktieselskab CVR: 37543128
Statsautoriseret revisor
Serienummer: 56c78f0d-d030-41dc-a7fe-ad94bcba5a88
IP: 185.98.xxx.xxx
2026-01-12 12:51:13 UTC

Mit ID